780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 9, Issue 4

Company Grade Officers:

A focus on their lessons learned and broad diversity of experiences

780th MI BDE
"STRENGTH AND HONOR"

Col. Matthew Lennox
Commander
Command Sgt. Maj. Ronald Krause
Command Sergeant Major

780th MILITARY INTELLIGENCE BRIGADE (CYBER), Fort George G. Meade, Maryland, publishes The BYTE as an official command information publication, authorized under the provisions of AR 360-1, to serve its Soldiers, Civilians, and Families.

Opinions expressed herein do not necessarily represent those of 780th MI BDE or the Department of the Army.

All photographs published in The BYTE were taken by 780th MI BDE Soldiers, Army Civilians, or their Family members, unless otherwise stated.

Send articles, story ideas, photographs, and inquiries to the 780th MI Brigade (Cyber) Public Affairs Officer (PAO) and The BYTE Editor, Steven Stover at steven.p.stover.civ@mail.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.

*__Correction__ in the last issue of the BYTE magazine, the author of "What Drives the Avenger?" is 1st Lt. Jeffrey Garcia and not Capt. Al Luna.

On the Cover

BUTLERVILLE, Ind. – Capt. Richard Shmel, a 17A, cyberspace operations officer, who hails from Eden Prairie, Minn., participated in the 915th Cyber Warfare Battalion's Field Training Exercise at Muscatatuck Urban Training, October 9, 2020.

The BYTE magazine's focus is on the company grade officers serving in the Cyber Branch. These young officers are the future leaders of the Information Advantage enterprise. Cyber officers direct teams of professionals and technicians that defend Army cyberspace and take actions against adversaries to ensure commanders' freedom of maneuver in the cyber domain. As leaders of Cyber Mission Force teams, Cyber officers are on today's electronic front lines, planning and executing defensive operations to protect Army networks and systems from attacks in cyberspace. They also plan offensive operations to disrupt and degrade adversaries' abilities to use the cyber domain.

To that end, we asked the Brigade Cyber officers to discuss the lessons they have learned and the broad diversity of experiences from the Basic Officer Leader Course (BOLC) to company command, from being a cyber planner and developer to being a member of a task force.

In line with the commander's intenet, we hope the articles herein spark the reader's interest and drive the conversation.

Praetorians! Strength and Honor

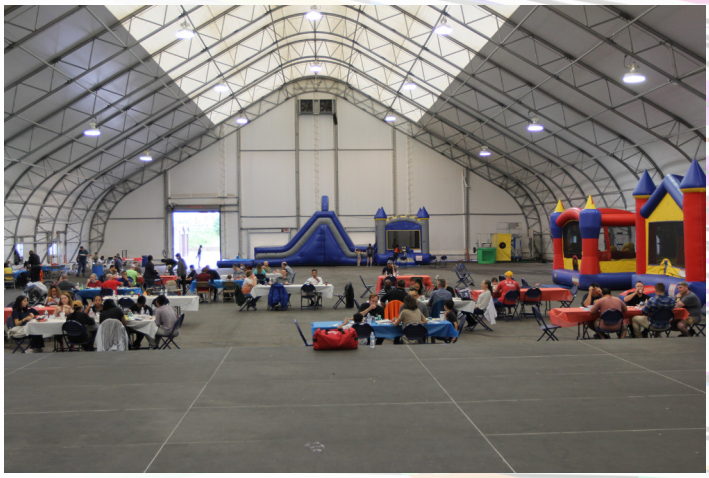
v/r,
Steve Stover
Public Affairs Officer
780th MI Brigade (Cyber)
Editor, The BYTE

Recipe for Winning as a Company Grade Officer

By 1st Lt. Brian Maguire, Battle Captain, Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber)

BEING SUCCESSFUL AS A COMPANY GRADE OFFICER is different for every role; however, the same principles apply to all of them. The Army is a people driven organization. Therefore, the easiest win is to always go to PT (physical training). PT for officers is not necessarily about physical training. It is where we can keep our fingers on the pulse of a unit. It is where we get to know our Soldiers. It is also where we get to hear the problems our Soldiers are facing. When we, as officers, hear these issues, we gain the chance to fix them since we have the rank to make drastic organizational changes much easier and quicker. When it comes to making these organizational changes, don't be afraid to throw a hail mary in what you ask for. The worst answer you are going to get is either, "no" or "let us table this discussion for a later date". Even if you are only having a morale event, see if the local community wants to let you use their facility or see if the MWR has a relationship with a business nearby. In the past, we have had professional sports facilities be entirely willing to let us do PT on their fields for free. Just be sure to check with the proper approving authorities before you execute.

Additionally, morale is paramount for our force to function at its full operating potential. Morale can make an operation scheduled for six hours take four (or at least make it feel like four) because people are having fun. Our organization is dealing with enough growing pains as it is, do not be the reason why your Soldiers are miserable. Your attitude towards the Army and the situation at hand is extremely contagious to those around you. Especially since, whether you know it or not, our Enlisted and Warrant counterparts are looking up to us. They look up to us not only in the lens of decision making, but



also through the lens of technical skill. As Company Grade Cyber Officers, we are typically the closest to the keyboard of any other officers, meaning we need to steward the profession of Cyber Warfare better than any other branch. We are the multi-headed drill that comes with batteries included and no need for a stationary power source. At our level, we all have a background, in the form of a STEM degree or training, that makes us beneficial to the mission. It allows us to make greatly informed decisions whether or not we, or our Soldiers, know the answer to the problem facing the team.

The final key factor in success as a Company grade officer is working with your peers to accomplish tasks. Whether you swing a backdoor deal that results in an exchange of favors, or you call up someone who just completed an event for their unit that your unit is now doing, working together leads to mission success. Not only does this take time and stress out of the planning phase of an operation for you, but the Soldiers in your unit will also ultimately benefit the most from the cross communication between leaders. If you, as the OIC (officer-in-charge) of an operation, sit in a "communication silo", your situational awareness is greatly hindered. Your Soldiers will need to work harder to cover down on your lack of awareness and the operation will inherently incur more risk due to not understanding the faults of your predecessors.

In short, the Army is a team sport where communication acts as the fence posts for our field goal attempts. It leads to greater moral, smoother operations, and a more capable fighting force. Cyber units become particularly lethal when that communication is paired with an in-depth, technical knowledge base at the Company Grade.

Path to Command: My Unconventional Journey to the 780th

By Captain Kyle Kiriyama, Commander, HHC, 781st Military Intelligence Battalion (Cyber)

IN MY THREE YEARS AS A CYBER OFFICER, I have been in three Cyber units across three duty stations. Spending my Lieutenant years as a Signal Officer, I realized that I wanted a different career path and changed branches as a Captain. I have been fortunate in both my duty assignments and locations. Throughout my time in Cyber, I have learned valuable lessons and gained valuable mentors along the way.

My first Cyber assignment was in the Cyber Protection Brigade (CPB) as a Computer Network Defense Manager. On a CPB Cyber Protection Team, I led the mission element with eight Soldiers and two Army Civilians. Our primary objective was assessing weapons platforms for cyber vulnerabilities. While conducting platform assessments, I had the opportunity to work with Armor and Field Artillery units. Following each assessment, we would brief our findings to the units' leadership. Although technical terms are common in Cyber, the Combat Arms officers' eyes glazed over like donuts. Often we work with other branches, I learned an important lesson, to be an effective communicator by speaking to the audience and finding common understandings.

Following the CPB, I was selected to be the Aide-de-Camp to the Army Cyber Command (ARCYBER) Deputy Commanding General of Operations. Serving as an Aide exposed me to the operational and strategic levels of command. I had the opportunity to work for two outstanding Generals with diverse backgrounds. Maj. Gen. (MG) Richard Angle, a Special Forces Officer, focused on transitioning ARCYBER from singular cyber operations to Information Warfare. Leveraging his unique experiences, MG Angle understood how to drive change and build a team. MG (Ret) Robin Fontes spent the majority of her career as a Foreign Area Officer. In her 35 years of service, she spent over 18 years in overseas assignments. Her ability to analyze problems, build connections, and integrate multiple organizations made her a force to be reckoned with across all domains. Although they had more time in the Army than I had in life, both general officers looked to me for my Cyber expertise. They listened and valued my input. In this, I learned that I should never discount anyone because of their age or limited Army experience. Each person can bring valuable skills and abilities to the table.

Upon arrival to the 781st, I immediately transitioned into command of HHC. My unique path taught me the importance of effective communication, driving change, building teams, and trusting subordinates. I have taken these lessons to form my command philosophy to remain flexible, be prepared, and take care of Soldiers and Civilians. ■

How to Effectively Train Operational Teams

By Capt. Al Luna, commander, A Company, 781st Military Intelligence Battalion (Cyber)

UNLIKE CONVENTIONAL OPERATIONAL UNITS, which cycle through red, amber, green before deploying, our Cyber teams are always operational and engaged. This persistent fight leaves us vulnerable to groups of Soldiers falling behind on training. This problem presents the question: how do we train teams and Soldiers in an operational environment? There are three parts of the training framework (FM 7-0) we can apply so a team can be operationally effective while simultaneously building the bench.

Planning

Part of the planning process is using Mission Analysis to help us understand how a team operates. Specifically understanding how a team develops and executes a mission package, what each section does, how each MOS contributes, and what problem set a team is aligned to. Mission Essential Tasks (METS) allow us to understand the requirements for a team to operate and which ones to focus on. As we look around the force, all Teams or Task Forces share common METS, but each team requires unique training geared towards their distinctive problem set. As our Cyber teams adapt to our adversaries and adopt new lessons learned, so does our training. By understanding the difference in operational training and organizational training requirements, we can blend them together to satisfy both operational and organizational requirements. Organizational training are the METS that provide a baseline of what a team needs to do to function and to effectively remission if needed. Operational training, like Malware or Crypto training, are team-focused and specifically aligned to that team's mission. The science of training is understanding all the METS required for a team to operate and building the training against those requirements. The art is building training that engages Soldiers, by using creative or interactive scenarios that increases a Soldier's ability to retain knowledge and, most importantly, reflects the operational environment.

Preparing

The Army has figured out training long before the Cyber branch was established. "Call for Fire" is doctrinally established, easy to train and simple to evaluate. The challenge we face in our branch is understanding new technologies and adversarial techniques to evolve our training. This is where the investment of training comes in. As leaders we must understand that while mission is priority, we also must allot time for our technical experts to train and mentor the new wave of Soldiers. I also see the challenge of building confident and capable leaders. While running Leader Professional Development provides overall knowledge on how to lead, nothing beats hands-on experience. When you integrate the 8 Step Training Model, you develop not only the junior Soldiers receiving the training, but also the NCOs, Warrants, and Officers. The experience of building, resourcing, executing training and assessing our troops is how we build leaders. So, we as Commanders must provide subordinates the freedom of maneuver to execute and give them feedback at each step of the Training Model. One of our goals as Commanders is to ensure we train operational teams that can conduct Cyberspace Operations. To accomplish this, backwards planning is critical. From top to bottom, we start with the Cyber Training Exercise (CTE). This collective exercise allows a team to be assessed and, most importantly, provides a space to execute their job from start to finish. Then we conduct section level training, focusing on the operations, intel, and planning sections. Lastly, we focus on individual training, which develops the Soldiers' ability to conduct specific tasks. Understanding this structure helps reach our endstate of qualified teams and ensures training is nested.

Executing

Even if we do all the proper planning and preparation, there may still be road bumps in the execution of training. Contingencies - such as bringing extra routers, spare servers, and even a redundant infrastructure (e.g. Local servers as the primary and a cloud solution such as PCTE as secondary) - prevents training from coming to a complete halt. Some Soldiers may need more entry level training while others may learn quicker. To ensure everyone benefits from training, prepare technical challenges with different levels of complexity. For any training to be effective, there must be an implementation of Training and Evaluation Outlines (T&EOs) which is what we use to train to standard. The T&EOs are the building blocks of how we assess a team, whether it's the proper use of tradecraft at the individual level or the evaluation of Mission Analysis for a team. Lastly, after assessments are completed, we can identify our deficiencies and retrain them.

While we can deep dive into the three parts of the training framework, this broad overview of each one provides enough for us as leaders to initiate movement and begin coordination for planning, preparing, and executing training. The end goal is that our training is well-structured, meaningful and creates qualified teams. ■

Avenger 6

Personal Growth as the Foundation for Teams in Cyber

By Capt. Conner Wissmann, B Company, 781st Military Intelligence Battalion (Cyber)

CYBER IS A DYNAMIC ENVIRONMENT with ever-changing requirements, tools, adversaries, and challenges. Despite the impact of COVID-19 causing the disruption of major commercial and service sectors over the last year, the Cyber Security industry has weathered this storm and is on a growth trajectory. The security market will grow by 14.9% over the next five years , catalyzed by the increase in the number and severity of attacks and increasing boldness in cybercriminal organizations. With the future relatively uncertain, the nation requires strong Army teams to react to and mitigate increasingly worrying trends across cyberspace.

Building a solid team capable of reacting to adversity in the digital arena is complex. No two Soldiers in the Army are precisely alike, but this can seem hyperbolic in Cyber: multiple work roles, levels of certification, and educational backgrounds create complexity in managing the team culture and individual Soldiers throughout their careers. But it is this complexity that matures outstanding teams, and diversity of professional experiences increases a team's capabilities against uncertain future requirements.

To support the development of our future teams, leaders and the organizational culture should support individual Soldier development. While this statement may seem counterintuitive at first glance, opportunities for personal development are often overlooked as one of the best ways to increase team unity. Individual professional development helps increase team capabilities and provides opportunities for Soldiers to mentor each other – bridging experience gaps and providing a foundation to grow as a team.

Increasing mentorship and cross-functional development should be a major focus area for our organization. Mentorship is a way to hedge against the uncertain skills that will be required for the future, increase team unity, and spur greater levels of career growth.

Personal professional development also increases team longevity by promoting retention; Soldiers who continually develop are more satisfied and less prone to negativity. Increased longevity, in turn, can increase a team's sense of pride in accomplishment, which can encourage Soldiers to create additional opportunities for development. Once the cycle of development and mentorship is established, our culture will continue to produce great teams for as long as it is nurtured.

Uncertainty in cyberspace is a certainty, and risks in our field are complex and numerous. The future demands great Army teams to mitigate and respond to these risks, and we are in a unique position to support the development of these teams as we move forward. Providing teams with the tools and opportunities to provide personal development can magnify an individuals capabilities and create an environment supportive of mentorship and growth. These environments are integral to fostering a culture where change is welcome, Soldiers are flexible, and teams can tackle the uncertain challenges of the future. ■

[1] (Facts and Factors Research 2021)

References:

Bibliography

Facts and Factors Research. 2021. Global Cyber Security Market Size & Trends Predicted to Exceed USD 398.3 Billion By 2026: Facts & Factors. June 21. https://www.globenewswire.com/en/news-release/2021/06/21/2250234/0/en/Global-Cyber-Security-Market-Size-Trends-Predicted-to-Exceed-USD-398-3-Billion-By-2026-Facts-Factors.html.

Cyber Operations and Developing a Culture of Learning

By Captain Joseph E. Kim, C Company, 781st Military Intelligence Battalion (Cyber)

AS LEADERS IN THE CYBERSPACE DOMAIN, one of our most critical jobs is to ensure that our Soldiers are trained to dominate in and through cyberspace. In order to accomplish this goal, we create systems and processes for training Soldiers to ensure that those skills can be passed on and taught to other Soldiers. This force multiplying technique allows the Army to train Soldiers to a certain standard and ensure that everyone is able to perform at that standard. In essence, the Army has a cookie cutter that it uses to create multiple Soldiers who are the same in terms of knowledge and expertise. This cookie cutter sits squarely in the institutional training domain. However, simply training Soldiers to a standard is not sufficient in the cyberspace domain as our jobs do not allow us to simply be replaceable cogs in a larger machine. In order to address this deficiency, AR 350-1 states that there are two other training domains: operational and self-development. It is within these two domains that we can most effectively develop a culture of learning.

The Army recognizes that the operational domain is where Soldiers will undergo the bulk of their development. As leaders, we must encourage our Soldiers to gain experience in the operational domain. Relying upon knowledge that they learned during their time in the institutional domain is not enough to remain in the fight against advanced persistent threat actors who are constantly changing TTPs (Tactics, Techniques, and Procedures) and improving their methods of attack. Specifically, encouraging Soldiers working as intelligence analysts to observe the fruits of their labor by going to an operation will allow for growth and a better understanding of the intelligence and operations cycle. This simple act of taking them to an operation shows them how their piece of the pie ties into the overall bigger picture. Such acts have helped to motivate Soldiers to learn more to better assist their teammates on operations.

Conducting cyberspace operations, however, requires a continuous upkeep of technical skills. Soldiers must train and apply their knowledge on a frequent basis. Becoming content with the current state of operations and technical expertise results in operational stagnation, and leaders must strive to inspire their Soldiers to constantly improve their technical acumen and think critically about the problem sets that they face. This is where the self-development domain comes in.

As we grow the Army's Cyber Mission Force, we will face this challenge of motivating Soldiers that have become complacent on a more regular basis. This challenge is an issue because it stops our Soldiers from innovating and ruins their appetite to learn more. In order to overcome this, leaders must emphasize that learning is a continuous process and does not stop with the submission of a JQR (Job Qualification Record) or the completion of an operation. So, the issue then becomes how do we motivate our Soldiers to overcome this potential complacency? We must give them the tools and the feedback to enable them to continue to refine their skillset. These tools include but are not limited to creating meaningful and applicable training (STTs) that directly support cyberspace operations, allowing Soldiers to take vendor training that is fun and will improve their knowledge, and listening to their ideas and trusting them to lead projects based on competency, regardless of rank. As we provide these tools, we must also provide feedback to assist them on how they are doing and encourage them to keep training and innovating.

In summary, Professor Schein of MIT put it excellently when he stated that "culture and leadership are two sides of the same coin." We, as leaders, must emphasize that learning is a constant process and one of the most critical aspects to cyberspace operations. As we do so, Soldiers will inevitably come to see that learning is not something that stops after getting certified or trained but a part of the culture that they belong to. ■

Leaders All The Way Down

By Captain Jacob Heybey, D Company, 781st Military Intelligence Battalion (Cyber)

There's a story that says a scientist, after delivering a lecture on astronomy, was confronted by an old woman, who said: "All of your theories are rubbish. The world is really a flat plate supported on the back of a giant tortoise." The scientist gave a superior smile before replying, "What is the tortoise standing on?" "You're very clever, young man, very clever," said the old lady. "But it's turtles all the way down!" (Paraphrased from Stephen Hawking's A Brief History of Time)

THE 780TH MILITARY INTELLIGENCE BRIGADE (CYBER) has a very top-heavy rank structure. This fact is initially surprising to newcomers, but the rationale behind it is apparent. Cyber units demand technical expertise acquired through either significant experience or long training pipelines. Therefore, any given Soldier within a Cyber unit must have spent the time to acquire that expertise, making it more likely that their rank is higher than the equivalent Soldier in a different unit. This line of reasoning makes sense as far as it goes, but our top-heavy structure has unexpected effects. Specifically, it clashes with standard Army expectations around "leaders" and "doers".

The Army informally divides its Soldiers into leaders and doers. Generally, commissioned officers and NCOs are leaders; junior enlisted and some warrant officers are doers. This dynamic plays out nicely in a standard infantry platoon. Out of 40 Soldiers, roughly 35 percent of them are officers or NCOs, leaving most of the platoon to focus on execution. But in Cyber units, we see a much more irregular structure. Manning varies widely between teams, but my generous estimate is that a Combat Mission Team or National Mission Team is 65 percent officers or NCOs: flipping the normal ratio of doers to leaders. For specialized organizations (like developer detachments), NCOs and officers might make up as much as 90 percent of the unit.

The ideal ratio of leaders to doers has not changed; we still need a majority of Soldiers to focus on accomplishing the mission while a minority focus on "leading", and all the additional tasks that come along with that. But our ingrained culture says that, by rank, most of our personnel should be leaders; and the mission suffers when the majority of personnel in a unit are expected to be leaders instead of doers.

Let's start at the beginning – what leadership expectations are we placing on our NCOs and officers? I think the vast majority of Soldiers within the Brigade have heard the "leadership speech". It goes something like this: "You are an NCO/officer now, so you are not going to be 'hands on keyboard' much. Your Soldiers will write code, execute operations, and analyze data. You are not a doer – you are a leader." I heard this as a brand-new second lieutenant at BOLC (Basic Officer Leader Course), and I've heard it reiterated to newly minted sergeants as well. Reactions to this speech vary; some are frustrated that they had worked so hard to achieve technical competence and are now being told they won't get a chance to apply it. Others jump at the increased responsibility and look forward to providing purpose, direction, and motivation to their Soldiers.

Of course, providing purpose, direction, and motivation are not the only parts of being an Army leader. Administrative tasks are attached as well; the company commander that neglects 350-1 training and incentive pay issues is not a good commander. So many commanders (and therefore their subordinate leaders) are judged on how well they track and handle these administrative tasks. But administrative tasks are not the only additional concerns weighing on a leader's mind. There is no shortage of working groups and status meetings for them to attend; no shortage of reports to write. Subordinate leaders must devote time to these meetings and reports to coordinate with other organizations and provide input on the future of the organization. Superiors must attend the meetings and read the reports in order to gather information about their subordinates' accomplishments and problems. Finally, units have training requirements and additional duties. Sergeant's training time is required; similarly, every company needs a safety officer, retention NCO, unit prevention leader, and motorcycle mentor. Somebody also needs to plan morale days and fundraising activities. All duties that must be filled by an officer or NCO.

All of these additional tasks have a tendency to land on not only the Soldier who formally holds a leadership role, but any NCO or officer. Adding more NCOs and officers doesn't help; the expectation

that the NCO/officer is leader, not a doer, remains. And administrative work has a way of expanding in accordance with the number of NCOs and officers available. In the end, we have more Soldiers doing "leadership" than we have Soldiers accomplishing the mission.

If that scenario seems farfetched, consider the following example: a cell is tasked with a specific mission supporting operations. This cell consists of a captain, a warrant, one staff sergeant, two sergeants, and one specialist. The captain, as the cell lead, attends all the necessary meetings, writes the status reports, and coordinates with other cells and external organizations as necessary. The staff sergeant is the cell NCOIC, so he spends most of his time curating a spreadsheet that contains everyone's personal information, 350-1 status, incentive pay status, promotion points, and evaluation thru dates. The warrant officer has the reputation as a technical expert; she is part of two technical working groups and is consistently asked to provide planning advice to commanders. One of the sergeants isn't qualified in his job role yet; he is in one of his pipeline courses right now. The other sergeant is behind on his concept of operation for his sergeant's time training. When he is finished with that, he is in charge of company fundraising efforts over the next few days. And after that, he is scheduled to sponsor a specialist at a promotion board.

And that is how we end up with a single, solitary specialist doing the work of an entire cell. It doesn't matter that the captain is an excellent programmer, nor that the warrant officer has 15 years of experience analyzing network traffic, nor that the staff sergeant does vulnerability research in his spare time. Their rank says that they are leaders, so they spend their time leading; the specialist is the only "doer" in the cell. Other units may not be so extreme, but the result is the same; there are more leaders than doers.

When asked about this situation, each NCO and officer provided very similar reasoning: "Going to these meetings and doing these admin tasks sucks, but somebody has to do them. If I take on the burden, my team is free to accomplish our mission." Admirable sentiments from dedicated leaders. Our specialist must be one of the best-led Soldiers you can find in the Army.

Our top-heavy rank structure combined with expectations about the duties of each rank makes for a skewed ratio of leaders to doers. Those with the appropriate rank on their chest are continually pulled away from directly accomplishing the mission and towards the various tasks expected of leaders. Some attempt to split their time between leading and doing. This rarely works – it's hard to solve hard technical problems in between meetings. We are left in a situation where we have more people reporting statuses than changing them; more people tracking 350-1 training than executing operations; more people planning the future of our infrastructure than using it.

Back to our anecdote: luckily for that cell, our specialist is the rare Soldier who is capable of approximating the output of an entire cell by herself. (Other cells are not so lucky; they face the unfortunate case where the Soldier with the most time to accomplish the mission is also the least proficient.) Of course, her work didn't go unnoticed. These kind of Soldiers don't stay in place for long; they get promoted (joining the ranks of "leaders, not doers"), or they seek out new challenges in the form of specialized units or training. Sometimes their expertise is the result of long experience and its soon time for them to ETS or PCS.

Whatever the reason, this cell no longer has a specialist capable of doing that amount of work. Their replacement is inexperienced or doesn't have the same expertise. So where are our doers? Who is writing code, executing operations, and analyzing data? What are our leaders standing on?

Nothing at all – it's leaders all the way down. ■

Leading or Reading

By Captain Orion Boylston, E Company, 781st Military Intelligence Battalion (Cyber)

AS THE COMMON SAYING GOES, "I CAME HERE TO LEAD, NOT READ." As leaders in the Cyber domain, however choosing one of these activities is not an option. Cyberspace is a vast domain, even diving into relatively small niches can lead you down rabbit holes that you would spend the rest of your career reading about. Just take one of the newest niches, cryptocurrency. Every day someone in the field of cryptocurrency comes up with a new way to transact, store or even launder their money. As leaders, this dizzying array of advancements and changes can lead to a choice: focus on keeping up with the technical aspects of Cyber, or focus on leading. Unfortunately, this choice is a false dichotomy. If we want to be effective as leaders we must learn to balance technical knowledge with everything that comes with taking care of soldiers.

First, let's discuss the need to be technically competent. There are some things that computers just can't do. Unfortunately, if you don't fully understand the complexity that can be present, you may think that some solutions transfer to different domains. Two things can combat this, knowing the fundamentals and asking the right questions. The first helps with the second, but failure in either can leave people doing circles around you while you try to figure out the basics.

The second aspect of being a leader is the people. If the moral case for caring about our people doesn't move the needle for you, then the cost benefit analysis certainly should. Simply put, if we don't take care of our people, then there won't be anyone left to do the mission. Taking care of people translates directly into those people staying with the organization and caring enough to take on more responsibility and look out for the service members that come after them. Too much rotation leads to training gaps that are difficult to keep up with, specifically in in work roles that can take years getting people into and through all the courses.

The task is certainly daunting. Being good at one facet is tough, but being good at both can seem intimidating. In our profession though, there is no room for error. Our adversaries are looking to exploit any weakness. ■

5 Pillars of Highly Effective Army Cyber Officers

1st Lt. Ademola Abimbola "AB" and Capt. Alexis Harper, HHC, Headquarters and Headquarters Company, 782nd Military Intelligence Battalion (Cyber)

IF YOU HAVE EVER BEEN TO ANY HISTORICAL PLACES around the world, then you might have seen a Roman Pillar. These triumphant vertical columns are structures dedicated to the strength and power of the Roman Empire. The very definition of a Pillar can be personified as, "a person regarded as reliable in providing essential support," but we would add one must also provide support for one's organization they are serving. Like these Pillars that have been erected over time, we will continue to build the Cyber force. The question remains what is the force looking for? To help you determine the qualities we believe a Cyber Officer must embody, we have created these five pillars of success: Decision Management, Emotional Intelligence, Reflection Management, Time Management, and Presence.

As you read through each Pillar below you will be given some examples on how one could strengthen your skills and harness your inner Roman Soldier.

Pillar 1: Decision Management

One of the traits that makes a highly effective Army cyber officer is the ability to make an effective decision. Decisions shape our identity and determine the future. A single decision can cause conflict between nations. Whether at the battle front, in a critical situation, or on the team, every cyber officer – from mission commander, operation officer, to company commander –faces choices each day and must make decisions. As a fact, the meat of an Officer's job comes from making decisions on behalf of the team or to our subordinates. It becomes a critical skill each time we take disciplined initiative. While preparing for Officer Candidate school, one of the quizzes that my then Platoon Leader asked me was "what are officers paid to do? I gave many good answers, but the best answer was decision making. Even in life, we all face choices every day. What makes a difference in our decision is the "children of the decision" – the result that comes after the decision is made. An effective decision maker will take responsibility and follow through until the decision is executed. The foundation of an effective decision is to have a good leadership approach. The following are tips to make effective decisions.

Knowing our boundary conditions and challenging the constraints: Boundary conditions are well known by mathematics students, but it is not a rocket science, some regard it as one of the toughest concepts in mathematics. A renowned management consultant and prolific writer, Peter Drucker, gave a succinct illustration of an application of boundary condition in decision making in his book "The Effective Executives". Drucker told a story of a New York power outage, a total black out in New York, and the New York Times had to rush to New Jersey to print. This constraint left the New York Times an hour and a half to publish its paper, but the executive editor and his subordinates started arguing about hyphenating a word in the paper. The argument lasted for 53 percent of the entire time they had to print the paper, because of this, only half of the work was printed. To most people, this sounds like a waste of time and energy, but the New York Times had the vision to be an impeccable standard for grammar in American English, so the decision was great, and they had no regret because the decision to print only half of the paper was in line with their values. In sum, no decision is correct if it does not meet the established boundaries conditions. Many leaders struggle with decision making not because they do not have the job skills but because they do not think about the boundary conditions – the core values, the culture, and fundamentals. Sometimes, it may be worthy to challenge the constraints we have when making decisions, such action may open room to explore other opportunities. In situations where challenging the constraints will deviate us from the boundary's conditions, then we reevaluate the risk.

Before action review instead of after-action review (AAR): The popular term AAR may do more harm than good if it is

not properly managed. If we analyze the outcomes of the AAR, sometimes there are few things that can be avoided if we do a holistic before action review – BAR. BAR helps keep track of potential pitfalls during execution, and an effective decision maker should consider BAR before execution. BAR helps to identify what needs to be solved and it helps to clearly identify the right decision. BAR put strategies in place to see the end from the beginning. In fact, BAR can help track our decision to ensure we see the expected ends. When we analyze the potential of a failing decision and its second and third order effects before execution, we are doing BAR. Sometimes, AAR is medicine after death when it is not preceeded by a holistic BAR. It is good to be convinced and stand by our decision, but it is not bad to weigh the option of its failure before we execute, this does not make a person a weak leader, instead it shows thoughtfulness in a leader decision making ability – analyzing the what-if in decision making sometimes helps to see the shortfalls in the decision. I call this a robust decision-making strategy. BAR would have helped the British government when they were concerned about an increase in venomous cobra in Delhi. The British offered a reward (money) for every dead snake, soon after this decision was made, people started to breed snakes for the reward. By the time the government discovered the flaw in its decision, it halted the incentive initiative, and the people had no reason to breed snakes anymore, and they started to release their snakes. This increased the snake's population. The same thing the government was trying to prevent eventually happened. If the government had done BAR, the second order effect might have been mitigated and reevaluated.

As leaders, our decision is as good as its execution. A decision that is not worth executing is not worth making. It is safer not to make a decision than to make a decision and not follow through the execution. A decision that is not acted upon is by itself a decision. Our team, peers and subordinates will not respect us if our decision is left unattended or unexecuted – Our decision must be actionable.

In sum, whether you are at home, work, or the battlefield, we all make decisions. The ability to make effective decisions is critical to our success as Army Cyber Officers. The test of quality decisions are boundary conditions, before action review, and execution.

Pillar 2: Emotional Intelligence

Currently, leadership attributes have evolved beyond the current leadership attributes in ADP 6 -22. In fact, one big trait that many leaders lack is emotional intelligence (EI). Emotional intelligence is the accurate utilization of emotional data to manage and balance one's emotions and the emotions of others to get better result in personal and professional life. It is interesting to see how we use intelligence from various sources to accomplish missions, but we never harnessed the power in our EI to shape us and become an effective leader. EI is a skill that makes leaders understand their own emotions and that of others in order to manage, relate and get better results. EI helps to make better decisions. Emotion leads to actions, and when it is combined with intelligence it helps to channel our mental energy in the right place at the right time. There is no reason to become a leader if our attributes cannot make a difference. Daniel Goleman has a favorite quote: "If your emotional abilities aren't in hand, if you don't have self-awareness, if you are not able to manage your distressing emotions, if you can't have empathy and have effective relationships, then no matter how smart you are, you are not going to get far. EI is an essential skill to have as a leader. It helps to shape our behaviors, increase our self -awareness, self-management, social awareness, and relationship management. Let's delve into some key concepts of EI and how it can help us to become an effective Army Cyber officer.

Self-Awareness: Emotions are contagious in nature and if not properly used, it can destroy things and result in irreparable consequences. Imagine a cyber-mission lead who is not aware of his attitude and reaction, this lead can potentially cause harm not only to his team but also the entire mission. A leader needs to know and understand his/her emotions and moods and the effect of such attributes on others. Self-awareness is the ability to see ourselves clearly, know who we are and how we fit into the world. Leaders with self-awareness live a productive life, such leaders are more promotable than others and are less likely to cheat or lie. Unfortunately, many leaders think they are self-aware, but they are not. Effective leaders know their strengths and shortcomings, they accept who they are and believe that those strengths and weaknesses are there for a reason – first, they work on their strengths that make their weaknesses less significant, second, they work on their weaknesses so that these weaknesses do not discredit their abilities and contributions as a leader. If a leader's weakness falls under character and integrity – these must be fixed before any other thing! One of the greatest CEO who is responsible for a drastic change in the history of Ford Motors was Alan Mullaly, he said "self-awareness is the single greatest opportunity for continued growth, performance, and improvement."

Self-Management: One of the things that make self-management a herculean task is our nature as humans – we are wired to emote first in situations that we find ourselves in. Self-management does not mean that you are doing things that limit your success, it means keeping the value and respect that people have for you. As leaders we need to manage our emotions and moods not just that, we need to control what we say and how we say things. We must not allow emotions to overtake us, leaders without proper self-management allow emotion to hijack their reactions and decisions. Self-management skill is critical as a cyber-officer. To simply put, self-management is the ability to self-regulate our impulses and moods to better serve us and improve our quality of performance on the stage of life. The greatest benefit of self-management is the ability to be a responder and not react-er. Research has shown that sleeping (tactically), reasoning and visualizing success in every situation help to have an effective self-management life.

Social Awareness: This is different

from self-awareness; it is an accurate understanding of your environment and people you deal with. Leaders need to understand other people's emotions. Asking people "are you okay?" when they seem down goes a long way to make their day. As leaders we need to be socially aware of the needs of others in our team and formation: leaders need to know how their words and actions affect people around them. This is not limited to only workspace, but also on social media. Effective leaders are socially aware of their environment. Effective leader does not give immediate response or assumption on what they don't agree with, instead they seek to understand people' s perspective and background and adapt their behavior to reflect the concerns of people on the team. Having a social awareness skill helps leaders to accommodate people, accept them for who they are. There is no better way to detect when people deviate from the norm than to have a social awareness skill. One of the United States' Army Generals who displayed this skill is Maj. Gen Cornelius E. Ryan: working with his Republic of Korean Army counterparts and using his social awareness skill, he transformed the Korean Military Advisory Group into the best military training and advisory mission. The following are proven skills that have helped leaders to become more socially aware: intentional presence, emphatic connections, know people by names and obverse body language

Pillar 3: Reflection Management

Not everybody likes the habit of the old people. Part of the reason why the old are wise is because of their ability to reflect on the past experiences. Time spent on yourself is never a wasted time especially when it is an intimate date with oneself. Disciplined reflection is about your awareness of rightful thinking. One of the qualities that makes an effective leader is the ability to reflect on self and experience. Reflection is not only a skill but also a tool. All effective Army officers have time to self-reflect. There is no point to have reflection if it will not shape our character, habit, and behaviors. Disciplined reflection becomes a waste of time when the product of the process is left unattended, only a fool will continue to act the same way and expect different results. Self-reflection is an important tool that helps us to gain insight on ourselves and from our experiences. One of my favorite quotes from John Dewey is "we do not learn from experience… we learn from reflecting on experience." Have you wondered why you keep making similar mistakes on critical issues or missions? The answer is simple – you have never taken disciplined time to reflect and learn from the act. Show me a wise leader, I will show you a leader that makes self-reflection a habit. The following are simple tips that can make self-reflection a life transformational tool.

Create Time to Reflect: As leaders, when we create time for self-reflection, we improve the quality of our leadership. And no matter the amount of excellence we cultivate, there is something or someone willing to pay us for what we are worth. One of the dividends of self-reflection is its application in our daily lives and seeing our performance in different work roles and providing outstanding leadership to subordinates and peers. One major enemy of self-reflection is technology, but that is only when you allow it to distract you.

Keep Journals: Writing your thoughts down is a good way to keep track of lessons learned from situations and events of life. And a proven and tested way to analyze a situation is not only by using the head but also pen and paper. Keeping journals brings intentionality into self-reflection.

Do Self Reflection: Seek a quiet place or plan to engage your mind as a first ritual in the morning. Think of events that you want to analyze or the role you played in certain situations, or you can even assess your value, approach, strength, perception, and interactions in certain activities. It may even be a decision that you have made or a failure you have experienced. The whole essence of self-reflection is to do critical analysis of self and ponder on where you think you can do better and be determined that the outcome of self-reflection will be used to make you a better leader. True leaders realize the need for help during self-analysis, if this is your case, then reach out for help and support. I have never seen any great leader who climbed the ladder of success by himself. Leaders of intent and purpose look for help where they may find it. After in-depth analysis of self, the next step is to channel and align the new self-discovery facts to your life goals and values. Self-reflection should make a difference in the way you speak and in general your approach to life, teammates, and co-workers.

In sum, not everybody has the patience to block time on the calendar to self-reflect, but at the minimum when we have situations and critical events around us, as leaders we should create time to reflect on them, otherwise we create more unintended consequences for ourselves. Effective leaders learn, grow, and make the best of every situation. It is prudent to say that self-reflection is not synonymous to self-depression. The bottom line is that everything happens for a reason, it is our job as Army cyber officers to access situations and events in our lives, and ask quality questions such as, what do these events and situations represent in my life and career, how does a particular event impact my leadership style, what critical life lesson can I learn from these events. It takes great effort to be an effective Army Officer, but the best effort is derived from how well we do self-reflection. Critical assessment of our actions and reactions on the stage of life and our leadership life goes a long way to make us the effective leader we desire to become. In asking why, we should be careful not to produce an alternative fact about a situation. Due to the regency effect, many people get too much into weed during self-reflection that it clouds their sense of self perception. Asking what question instead of why question will help to streamline and gives the best lesson from any event or situation. As you engage in self-reflection, journey guides your heart. It would be remiss not to say that self-reflection is not necessarily a retrospection, but the former is worth our time because of the insight it produces.

Pillar 4: Time Manaagement

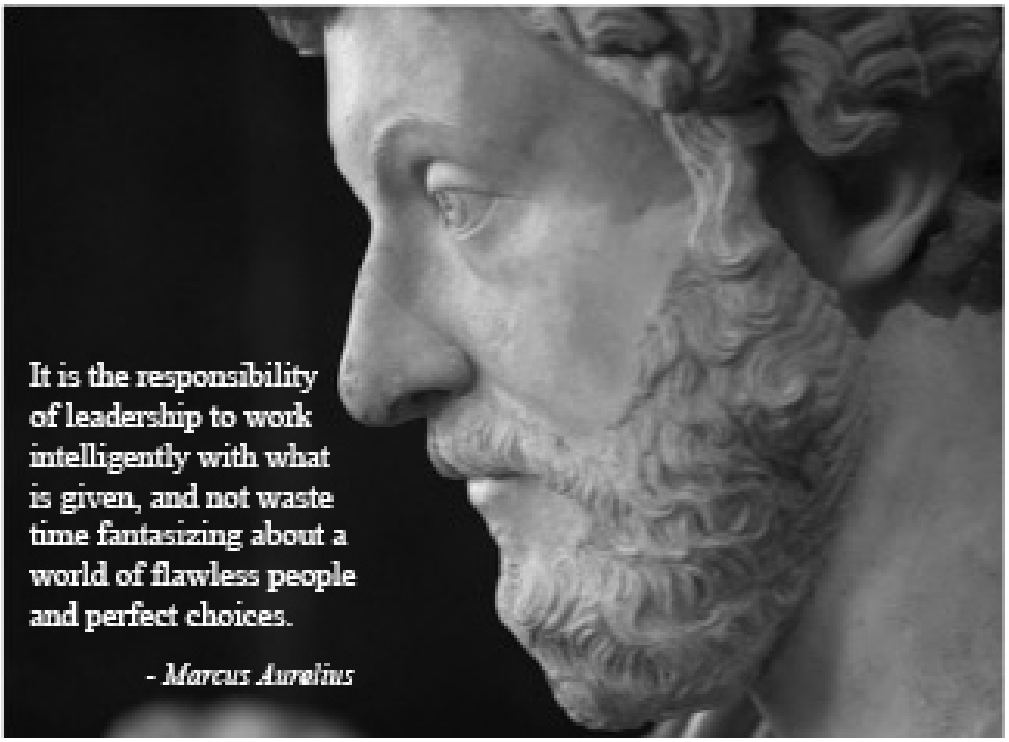
If you ever attended one of our officer LPD's you will discover a trend. We always end up discussing some aspect about history or a book that someone recommends everyone reading. On one of

the many research missions we discovered a chap named Rory Vaden. He wrote a book that seemed contrary to everything we are ever taught as an officer, the book was called "Procrastinate on Purpose". The premise he shares is, "there is no such thing as time management, there is only self-management," and "time continues on regardless of what we do, so all we can do is decide what we will be spending our time doing or not doing for that day." If we could summarize Vaden's tips on how to self-manage your time better then maybe we can start managing time better as a Cyber Officer. The first thing he says is to eliminate tasks where you can or say "no" if your plate is already full. Second, try to automate aka create a script for things when you can if it makes sense. Third, delegate by teaching others how to complete a task, but remember they won't be perfect without practice so be patient. Third, procrastinate or delay an action on purpose IOT make a better decision because sometimes timing is everything. Lastly, don't forget to concentrate on the tasks that are priorities, everything cannot be a priority so you have to learn to determine what is. Time is after all a resource that cannot be replenished so use it wisely.

Pillar 5: Presence

If you look at your OER you will find that "Presence" is an aspect as an officer that you are all being "graded" on. Your ability to be professional, confident, resilient, physically fit, and your overall mission command are all aspects of this. Marcus Aurelius, a great Roman leader, lived around 100 AD and became one of the most powerful Roman Emperors with the largest military. According to history he did not even begin his career commanding the military until he was in his 40's. Often when you think of a general commanding an army they have many battles under their belt, but what Marcus lacked in experience on the battlefield he brought stoicism in spades to the table. The basic idea of stoicism is that you develop skills of overall self-control, manage your emotions well, and can remain calm in stressful situations. These attributes become incredibly useful in war and during crisis situations, which is why this philosopher thrived as a general of one of the largest armies. The biggest key to success for a stoic person is not setting yourself up for failure by expecting yourself to succeed every time. Marcus would encourage you to "have power over your mind – not outside events. Realize this, and you will find strength". As a leader we must remind ourselves that we must be the calm in a storm, evoke the right emotion when necessary and be a positive leader that does not drag one's people down. How you present yourself as a leader could very well be the difference between successes or a failure of any mission.

Hopefully after reading through these Pillars there are moments of reflection. The hope is that we all continue to self-reflect and improve ourselves daily, but you can take it one pillar at a time. Remember a pillar in the physical world is not just a kick stand made from marble, a pillar is the strength and foundation that will ensure the tests of time of any structure built on it. If you want a good, strong foundation then you must adopt these 5 pillars and make them the core of yourself as you continue to grow in Cyber as an officer. Identify the pillar that you are missing and work hard to practice it. Perfection is only achieved through intentional practice.



Navigating Uncertainty

By 1st Lt. Alex H. Day, Operations Officer-in-Charge, A Company, 782nd Military Intelligence Battalion (Cyber)

COMPANY GRADE OFFICERS in the Cyber Mission Force are thrust into positions of authority, often with little experience. They must act as leaders, planners, and communicators in a field where the state of the art constantly changes and in the face of a Byzantine corporate culture. Not every effort will be successful, but by adopting lean and aggressive approaches we can execute more fault-tolerant plans.

The Cyber domain presents a system of deep complexity. However, engineers and technicians have long developed predictive models in other sophisticated fields. Look no further than aerospace manufacturing or commercial nuclear technology where it's not uncommon for thousands of components to interact. One is challenged to understand the system's internal dynamics, which often behave in unintuitive and nonlinear ways. Cyber presents similar challenges, where networked devices with varied and inscrutable configurations hamper the development of practical models. Furthermore, in an ecosystem where vendors and community developers rapidly upgrade, even robust plans are tested. Additionally, the Defense Enterprise's own bureaucracy adds considerable lead times to otherwise straightforward tasks. In an institution dedicated to advancing national interests through Cyberspace Operations we rarely have the capacity to embrace the comprehensive methodologies that model sophisticated technological entities in more established industries. Where legacy domains like aerospace and commercial power work at timescales of years or decades ours must adopt rapid, iterative techniques to deliver results that are timely and relevant. The following are lessons learned I would encourage junior leaders to consider.

Identify the Minimum Viable Plan

To paraphrase an engineering adage: "When you've removed as much as you can and your product still works, it is complete." It's easy to enchant ourselves with feature-rich plans or become sentimental about the work put into what will become stubs or dead ends. Distill your efforts into a handful of overarching, executable tasks and wherever possible advocate for the simplest means of achieving it. Complication introduces fragility – ruthlessly cut down distracting or unnecessary features to better steward resources and achieve greater flexibility. The quality of a plan is not measured by whether it was executed precisely as written, but rather whether it provided sufficient flexibility to accomplish mission in the face change.

Strive to Be as Lean as Possible

While collaboration is laudable not every organization has a customer-centric approach. As the tactical element, Cyber teams are on the hook to deliver tangible results on behalf of their higher headquarters. Understand that as the number of stakeholders increases so too does the overhead of coordinating these elements in concert. Practically speaking, never be afraid to ask for help but heavily scrutinize resource requirements which are not organic to the team.

Determine What Doesn't Work Early On

You will almost never have the luxury of fully understanding a problem before you must make a decision. Days or hours will be the difference between success and failure. Much can be said about the aggressive pursuit of plans but the takeaway is that it's far easier, and cheaper, to fail early in the process than take a project to culmination only to discover it's no longer feasible. Relentlessly getting after it grants opportunities to identify weaknesses and iterate early in execution. Seek to drive down staff hours and resources dedicated to plans that will not bear fruit.

Have Failure Criteria

Joint planning establishes termination criteria for the cessation of hostilities. Although couched in terms of fulfilling objectives leaders must be ready to make impartial, and at times sobering, calls. No leader should anticipate failure but we must nonetheless construct testable criteria to determine when an existing course of action is no longer viable. These provide benchmarks that decision makers can use when electing to continue mission, execute branch plans, or restart the planning process.

Sink or Swim: Cyber Officers Tossed in the Deep End

By 1st Lt. Dominic, J. Pontious, Operations Officer, Combat Mission Team, D Company, 782d Military Intelligence Battalion

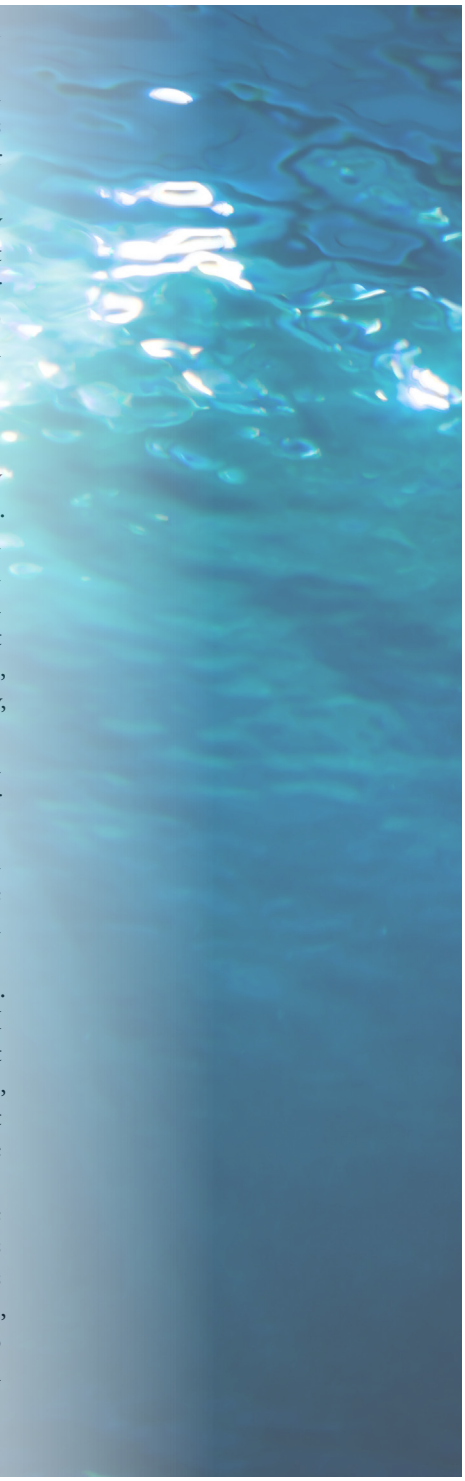
TRANSITIONING FROM BEING AN ENLISTED SOLDIER in a U.S. Army Forces Command unit to a Company Grade Officer in the Cyber Branch, I find myself and my peers to be in a uniquely difficult and at the same time rewarding position. This difference becomes especially apparent when I compare our experience to my peers in other branches. Training aside, I have spent my relatively short time as an Army Officer as the Operations Officer for a Combat Mission Team (CMT) and have found there are a handful of lessons learned and experiences that are shared among the branch. I do not claim to speak for everyone. I only note what I have seen or heard among my peers and coming up from my subordinates.

The first point I make is foundational to the points that follow. Cyber is a young branch when compared with any other in the Army. This means we do not have the strongly rooted and firmly established traditions and guidelines a fresh Company Grade Officer would find in any other branch. I have found this to be both a blessing and a curse. We are afforded the incredibly unique opportunity to establish our personal leadership style befitting our subordinates and our situation. Conversely, we do not have the tradition to fall back on when confronted with trying situations. There is simply not the precedent set for us. We can both sail our own path, but also find ourselves lost at sea when confronting the sometimes very tough decisions within the cyber domain.

Building from this foundational premise, we find Company Grade Officers not falling into traditional roles as happens in other units. Specifically we are not paired early on with a senior Non-Commissioned Officer (NCO) in the role of Platoon Leader and Platoon Sergeant. We do not get this time and opportunity to absorb many experiences and hard won knowledge beyond our own as many of our peers do. We find ourselves often finding an NCO to fill this role for us, usually within the specific path we are hoping to pursue. My advice to any Officer or NCO in the field that has not yet developed this unique almost mentor mentee style role, do so. The relationship is nourishing in both directions and strengthens the Army at every level.

Thirdly, growing upon the unique structure of Cyber, the technical nature of our branch encourages a hierarchy squished format at the Company Level. We tend to do away with traditional Platoon and Squad breakdowns for all practicalities. This encourages technical knowledge and discussion of the difficult technical problems is not stymied, which is a good thing. Consequently, Company Grade Officer must engage with subordinates and their superiors in a manner that is not taught to us in our traditional commissioning sources.

This leads me to the final two – and in some ways a single – lesson learned. The Cyber Branch carries with it an expectation of technical understanding and expertise this is not common in other branches. Without a strong technical foundation I have found it can be frustratingly difficult to communicate with subordinates, peers, and supervisors alike. This lands me at my final point. It is critical to learn the fine line between technical excellence and not taking work home with you. The technology within the Cyber Branch is ever developing and growing. There is always more to learn and understand, but we do not always have more time to dedicate with family, friends, hobbies, and other pursuits.



Junior Officers' Perspectives in a Joint-Combined Environment

By 1st Lt. Danielle L. Jaksha, Operations Officer, and 1st Lt. Jordan P. Morin, Operations Officer, Detachment Hawaii, 782nd Military Intelligence Battalion (Cyber)

FIGURING OUT WHERE YOU FIT in a joint-combined environment at your first duty station can be like drowning if you don't have someone to teach you how to swim. When asked "who's your boss?", it's like a multiple-choice answer where "all the above", "only A and B", or "none of the above" are all correct answers depending on who's asking. Luckily, we had the best team to show two lost lieutenants the way. We are 1LT Danielle Jaksha and 1LT Jordan Morin, BOLC (Basic Officer Leader Course) classmates who posted to paradise at the same time. While BOLC taught us how to Cyber, no course could effectively prepare us for the symphony of chaos that is a combatant command level joint-combined exercise.

Pacific Fury and Pacific Sentry are combined exercises held at United States Indo-Pacific Command (USINDOPACOM) that test its component's ability to fight a nation state in multiple scenarios. All facets of the combatant command to include cyber come together for the 10 days and are thrown into an orchestrated crisis. Both exercises stress tests the processes that USINDOPACOM and its components have in place. Pacific Sentry adds an additional flavor in that the crisis is fought together with a Second Party Nation. This forced us to coordinate assets and synchronize fires in all domains with every component of another nation.

As new lieutenants who were just starting to learn how offensive cyber functions at the team level, we came into the exercise ready to make mistakes and absorb as much information as possible. As part of the Cyber Operations Integrated Planning Element (CO-IPE) we were motivated with our limited experience of coordinating cyber operations at both the strategic and tactical levels. Unfortunately, we quickly came to a realization that everyone outside the CO-IPE had an equal amount of cyber knowledge and experience. It was often found that cyber as a whole was misunderstood or under-utilized. For example, tactical leaders and component commands did not understand the difference between the various cyber authorities, operations, or how long those processes take to become fully developed and executed. This created friction between cyber and the other components within the exercise as we spent a majority of the time explaining our process and by the time tactical commanders understood how to request cyber operations, a majority of targets had been physically destroyed and the exercise was coming to an end. It seemed as if "cyber" was a foreign language. At the same time, when we finally started getting requests, it was clear that the requestors did not understand our capabilities and their intended effects within the battlespace. Tactical leaders would try to press the big red cyber button and yell "Go Go Gadget cyber!" when the desired end state was infeasible with kinetic assets. These requests were simply impossible and we did everything we could to explain how cyber operates to ensure there was a clear understanding of what we could and could not do in future engagements. As motivated as we were to tackle the problem set and contribute to the Task Force Commanders objectives, the reality of offensive cyber is that we don't interact with tactical units and component commands enough. These exercises throw cyber into a crisis engagement when in reality we are the most effective beforehand, in Phase 0. We bring the persistent engagement months before the crisis in order to help shape the battlespace and inform leaders. The time to practice these interactions and set expectations should not be first happening at such a high level exercise either, that should be the time we test and strain those relationships. As Junior Officers we must continue to educate our peers in other domains on what we bring to the fight and how we can be most effective.

Guidelines from an Outgoing Captain

By Capt. Raymond M. Goldberg, Plans OIC (officer-in-charge), Detachment Hawaii, 782nd Military Intelligence Battalion (Cyber)

AS A BRAND-NEW LIEUTENANT, it can be intimidating to start your career on the OCO (offensive cyberspace operations) side of the house. This is especially true for Combat Mission Teams and Combat Support Teams (CMT/CST), who have multiple variables that exacerbate the difficulty of "learning on the job". As a Lieutenant in almost any other branch of the Army, you would have had access to a multitude of established SOPs (standard operating procedures), a highly effective higher headquarters (HHQ) staff giving your team purpose and direction, and decades/centuries worth of professional development material. In DoD Cyber, you will be lucky to get one of these.

I am Captain Goldberg, and my purpose for writing this article is to give new Cyber Officers some guidelines to follow in general, but particularly within CMT/CST's problem set.

1. Don't Get Discouraged

I know this is horribly cliché, but this guideline is especially true in Cyber. You are walking into a world that is built from the ground up to confuse and frustrate newcomers. Being in the military only intensifies this effect. Between the contrived ADCON/OPCON structure, the confusing (and sometimes contradictory) orders/intent of HHQ, the large amount of context for what's currently being worked on, and the more experienced Officers' innate desire to speak in acronyms; it's all enough to make you want to give up.

For the sake of our profession, you can't give up. You have to keep asking questions, requesting which SOPs/documentation to read, and otherwise challenging the purpose for why we do things. You must strive to understand why we are the way we are, in order to eventually turn us into something better.

2. Keep It Simple, Stupid

This guideline is one that you will inevitably break, but you should try to always live by as an Officer. Since you are the one in charge, it is your responsibility to come up with a plan for how your sub-element/Line of Effort (LOE) is going to get the job done. This responsibility is made more difficult due to lack of SOPs and documentation, so you will have to rely heavily on your leadership's past experiences and your creativity. At the end of the day, you will have to choose a plan that makes sense to you and your team.

My advice: keep your plan as straightforward as possible; the less moving parts there are to it, the better. Only go with a complex plan out of necessity, not out of preference. Never forget your # 1 job as a leader (operationally): provide purpose and direction to the team. Making sure your team knows where they are and where you plan to go with them will be your main concern. While you will usually have about three other tasks to complete on a day-to-day basis, they will never be your primary task.

3. ***When all else fails – row, buddy, row…***

To be honest, this is a guideline that I often forget and must learn over and over (and over) again. During your time here, you will eventually learn other people's jobs. You'll learn how the staff at our OPCON headquarters work, for better or worse, and you will develop opinions on how they should change. You will get frustrated about how long things take, how risk-adverse people are, and how nothing is as straightforward as it should be.

I am here to tell you that your feelings are valid, but ultimately unhelpful in the moment. If you were General Nakasone for a day, I am sure you would be able to fix everything wrong with USCYBERCOM, and we would be just fine. But right now you are a junior officer with very little power, and your singular duty is to take care of your team. Focus on doing your job to the best of your ability. Don't get weighed down by what others should be doing; that is their concern. Do what you can in the position you were assigned – no more and no less.

So, when you look around and find that everything is going wrong, and you and your team are being swept up a creek that you never intended to go down, the best thing you can do is grab an oar and row, buddy, row. ■

Being the MiTM

By 1st Lt. Jennifer Alvarez, A&P OIC, Detachment Texas, 782nd Military Intelligence Battalion (Cyber)

AS TODAY'S ARMY SHIFTS TO A NEW GENERATION, Company Grade Commissioned Officers face a tough role ahead for the foundation of what the Cyber Force will be. As a first-generation Cyber-Officer, one must form the bridge between the Senior Leader's intent for the operation and to understand the Soldiers they have within their team. Previous Army culture has shown a different mentality of Soldiers with a linear battlespace terrain. However, as the adversary adapts, so does the forces we lead into battle adapt. Regardless of the type of battlespace, certain principles remain such as to win on the battlefield by achieving the maximum effects of fires by being smarter and better than our opponents. The way to achieve this is to understand the different leadership requirements at different levels and that the use of teamwork among the different levels holds a huge impact on that effectiveness. Commanding Generals and Field Grade Officers in the Cyber Force were produced from other branches within the Army which preserved the principles of Strategic Planning while giving the Company Grade Officers the ability to focus on the tactical planning while simultaneously learning the strategical side as well.

As a Company Grade, I have seen both sides of the critical planning requirements of higher echelon Commanders while also relating to the new generation of Soldiers who are not familiar with the traditional Army culture of most historical units. By being in the middle, one can view the perspectives of both the senior leaders' goals along with understanding the Soldier's mentalities. In order to unify the team to exceed the requirements of any given tasks at hand, one must be able to apply certain skills taught by traditional Army culture into a technical environment. However, my experience as an enlisted Soldier has taught me that our Cyber Soldiers do not respond in the same manner as other Soldiers which gives the leaders the opportunity to shift those concepts to build their subordinates' skills, will, and teamwork.

Certain concepts that could be modified include adopting a leadership style that reflects your team. A leader can't assume that what's right for you will be right for your team. One's specific leadership style may not work with members of the team and could cause them to become despondent. By adjusting one's leadership style, it allows the leaders to be more successful while also building the next step of trust. A key responsibility of a technical leader is to build meaningful relationships and establishing trust with its members. This will incur higher success levels for achievement by developing a sense of responsibility in your subordinates which stretches out their ability, potential, and skill. However, by entrusting one's subordinates, Company Officers need to also be able to take ownership and responsibility for the mistakes and flaws that may occur from the team. When a deadline is missed or a project doesn't work as planned, getting it fixed is a top priority, not pointing the finger. Leadership is about people, so genuinely help people grow and do their best job will make you the best leader you can be.

Most people in an organization want to know how they can help the team to achieve its strategic visions, and be updated on the progress towards it, which leads to leaders needing excellent communication skills. Our job as company grades Officers is to understand the project and then explain it to the team while doing it in such a way that it motivates them to want to work on it with clear and concise guidance. Distill the bigger picture in a way that's actionable and personalized to your team as each member offers a specific skill whether analytics to software development, one needs to find the proper communication style that works best for the team. In order to find the proper leadership style and communication methods, one needs to evaluate themselves. Look at good leaders around you and then look at yourself honestly by asking what can I do to be better? Study different forms of leadership whether good or bad and learn to turn one's weaknesses into strengths. By adopting these concepts into a technical environment, Soldiers can expand on their abilities while also becoming the technical and tactical leaders the Army needs them to be, which will help senior leaders accomplish the vision and direction the cyber force is moving towards. ■

How I got everyone to listen to the XO

By 1st Lt. Cristobal Ibanez, HHC, 915th Cyber Warfare Battalion

THE 915TH CYBER WARFARE BATTALION is a rapidly growing unit with over 200 personnel assigned as of August 2021. While we are still small comparatively to other units – the 915th is expected to grow to over 600 people in its full capacity. Currently the biggest company is the Headquarters & Headquarters Company (HHC) with more than 100 Soldiers with more on their way. I took over as the XO (executive officer) in May 2021, just in time for HHC's first change of command. Although, a lot of the groundwork had been laid for the company before my arrival one of the major challenges for any organization in its infancy is that there is always too much work to go around and not enough people to do it.

One of the advantages of being a small organization was that communication was simple and direct. Initially, it wasn't hard to reach out to everyone in each headquarters' section – that was until we started growing. Our growth has outpaced our lines of communication and will soon outpace more of our resources. While the answer many may suggest would be to just "use the chain of command" the solution quickly falls apart when we consider the unit is currently spread out between six different locations with milage between each building. We have identified it as a problem and I foresaw that it would continue unless it is actively worked on in perpetuity. While it would be easy to recite all of ADP 6-22, it does not state how to fix communication in the middle of a pandemic. I started by taking note of the information flow in the unit and that was when I noticed I was the one of the people who was not actively informed. My experiences and best strategies that I currently use started from the moment I tried to coordinate things as a newly appointed XO and failed disastrously. It failed because I overestimated my communication skills. I learned that bad communication could be worse than no communication. It becomes counter intuitive to the desired outcomes. Usually it originates from one of the following three: lack of relevant detail; poorly worded sentences that resulted in confusion; and the presentation of information caused people to lose interest and dump the information. I quickly had to redefine what good communication was and start to take a different approach to the way I was doing business.

I first had to become a "bank" of information before I could start to spread my agenda and complete assigned and implied tasks. As one of the leaders in the company it is imperative to have general awareness of all events, people, and tasks taking place in any given week. It helps to identify gaps and conflicts early in the planning process; it saves time and avoids the stress of having to de-conflict anything at the last minute. One of the best ways I learned to become situationally aware was to become a "bank" of information. It becomes simple transaction process, I become a source for people and I bank any information I ask for or want to know more about. The more I could be the source of answers for people the more they would engage with me and add to the bank. However, it is a rigorous strategy that requires extensive note taking, since it is next to impossible to keep that much information in one's head and still be accurate. I often still find myself melding two pieces of information that are unrelated into a mess of bad unhelpful information that does more harm than expected. To add more challenge to the strategy; all information collected has a shelf life and because time doesn't stop, the relevancy of information depreciates overtime. This means most of the equity gained is lost when I am away from the interactions that happen within the company. An unfortunate side effect is the added stress that comes when I go TDY or on leave because of expiration of all the valuable information I had at the time. To leverage the supply I do have, I must quickly find a way to spread and disseminate the information. The demand of the information supply is driven by those affected by it. By taking note of the audience of any piece of information I can quickly determine the value of it. This allows for the prioritization of the information and how much effort I use to keep it accurate and up to date. The delivery of the transaction is important to sustain a good standing with those that come looking for information. As is in standard practice, keeping it to the five Ws at a minimum creates a perfectly well packaged message that works in a fast-paced environment. Depending on the person, most people don't have the time to listen the opinions or irrelevant information you might have and is something to keep in mind when engaged with a client. It is also important to keep it fair with the information you ask for as to not tax the person too much when bombarding them with questions, but as a "bank" it is always important to take just a little more than you give. In a quick summation it is all about relationships. Managing relationships takes effort but the reward always pays off otherwise, the alternative is to be placed out of the loop and that never feels good. As a leader in the company, I also must spread the information I collect which becomes the hardest part of the job.

The information flow quickly becomes a mess when trying to pass accurate information in a timely manner. It becomes hard because it is out of my hand for the most part. However, I still have the power to influence it based on how, when, and who I choose to disseminate the information to. For most situations and standard practice around the Army is the chain of command, however, as mentioned before, as a rapidly growing unit we're currently outpacing established norms. The culture at the unit is still developing

and I expect it to change overtime as things become addressed and processes become established. Most people in the unit also recognize that we have an easier time shaping the culture because of the reasons just mentioned. Unfortunately, I do not see this being leveraged as much I would like to see it, but I am not discouraged with doing my part. From my point of view, I believe the people in the unit to be more junior. We take in a lot of gains who are brand new to the Army and have come to the 915th is their first unit – to include myself. While it may be a result of remote learning at the schoolhouse and also while I probably may only speak for myself – the learning curve of starting and maintaining relationships at my first unit was rather tough to put it simply. These brand-new people still have to take time to develop their interpersonal skills and so the process of developing relationships will be slower. To add to that, by packing over 200 strangers into a unit with more continuously arriving each week over a short period of time, it is safe to say that these relationships will take time to mature. Fortunately, I am quickly coming up on the one-year mark at the unit and I am at a point where I can leverage the relationships I have established.

The people I use (beyond the chain of command) to spread information are my conduits. They are the people I can trust to spread information in a timely manner and can leverage their relationships to a large group of people. These people have a level a credibility that others trust with what they say. The people I prioritize last are my dead-ends, or the people I have identified where the information flow stops. They are how I measure the effectiveness of the current information flow, if its not getting to them – then I know there is a gap I must find. By using my conduits and dead-ends I mentally build out the spheres of influence and branches of information flow within the company. This is the strategy I use on an individual level; the other two I use are small group engagements in person and addressing all personnel in the company. With those techniques in place I overtly use redundancy. While it may seem like unnecessary extra work to put the same information on various different platforms, it is imperative to do so if I want to reach everyone. One of the tools I use is the weekly newsletter I send out by email. I carefully choose and strategically pick what information goes onto it and what can wait until the following week. I do so because, people tend to skip long emails that are laborious to read. By keeping it minimalistic, simple, and with high value information I can expect more visibility on it. A tool we use output quick updates – typically afterhours – is the Signal Chat instant messaging app. It is useful for its group chats and has an added bonus of providing a quick way to collect phone numbers without creating new contacts for everyone in your phone. The third platform we are beginning to use is the A365 Microsoft Teams. It is the best platform for centralized information that is slow to change and is the best way for everyone to be reminded and continually informed. However, it involves a level of personal responsibility for those who wish to stay informed. I believe this powerful tool is the solution to most people's problems that most people never asked for. It is a more permanent solution to CVR Teams, but wildly less popular than CVR, because A365 is CaC enabled. Unfortunately, that extra small effort to sign in is enough for people to completely disregard using it, no matter how much I push it. The second major reason most people don't use it as much is the impracticality of using it on their personal mobile device. However, even with these tools, talking to people in person has always worked the best for creating a shared understanding within the company. It also comes with the risks for miscommunications. Miscommunication is the result of misinterpretation of one's message. These misinterpretations stem from the physical limitations of one's speech and ability to hear or listen. My major pitfall comes from my ability to articulate my speech patterns, I usually become too soft spoken or speak too rapidly for anyone to understand me. This gets amplified by noise pollution in the environment I'm in. Daily speech practice and active voicing helps mitigate some of these physical limitations, but the risk will always be there. A miscommunication can delay or even halt some of the most planning done for any task. Actively fighting against It is the most critical piece for effective communication.

While I still haven't gotten everyone to listen to the XO, there has been a noticeable improvement across the formation. As I continue to work and refine the techniques I have learned, I am confident that I will reach my goal. I learned that always being situationally aware makes me a conduit for other people. It helps me plan quicker, more efficiently, and helps me identify problems before its too late. I learned that personal responsibility is something that everyone owes to themselves. Afterall, it is usually our choice to stay informed and participate. By relying on dependable leaders, we can make an effort to motivate soldiers to choose to be a part of the unit culture. Know what tools to use to reach a wider audience and being strategic with how to use to keep them engage is critical for permanent in lines of communication. However, being agile with how you engage individuals is equally important and serves as the bedrock with creating and solidifying relationships. We still face plenty of unique challenges and I anticipate many of the techniques used will change and many more will be created. I will always try to keep myself informed with what is around me and my goal is to have everyone informed on a daily basis. This is how I will provide purpose and direction to my company. ■

Networking – An Ambiguous Term for the 17-Series Officer

By 1st Lt. Kurtlynd McLane, Cyber Planner, Expeditionary Cyber Team, 915th Cyber Warfare Battalion

"THE BATTALION COMMANDER just came by; did you get to meet him?" I looked at my team lead, defeated that I am running a trace route for the third time during a capture-the-flag exercise. "No, I was trying to figure out where these packets are going." It was frustrating that I was not networking because I was looking at this network. The bane of introverts on one hand but a technical understanding in the other, only a balanced combination of the two produces a valued 17-series officer. This is the steepest learning curve I tackled amongst the other challenges during the start of my military career as an officer in the Army's newest branch.

I start my journey into cyberspace with Cyber Basic Officer Leader Course (CyBOLC), the longest of its kind at nine months. One of the great benefits of CyBOLC, aside from the prolonged assignment to TRADOC, is the technical training. The curriculum at the time included, Python programming, CISSP, and the infamous Cyber Common Technical Core (CCTC), all of which lasted four and a half months. While the knowledge gained was invaluable, it was during CCTC most lieutenants found what side of the fence they were on. "Leadership is the process of influencing people by providing purpose, direction, and motivation" (Headquarters, Department of the Army, 2012). Most of the class quickly learned to appreciate that they were great at influencing; the rest of them graduated at top of the class. This was, for many, the first exposure to a dilemma that is being a Cyber Officer.

Our class also faced an entirely new challenge; a pandemic swept the country, and we became the impromptu pilot class to start distance learning. What was our first course? CCTC. If learning how to reverse engineer was not hard enough, doing it remotely made it tougher. As many students can attest, this was an uphill battle, especially with poor Wi-Fi. Fortunately, the Cyber Training Battalion and some great NCOs provided great support. Aside from a server shutting down in the middle of testing, the remaining sections continued error-free, given the circumstances.

We would continue in this manner until graduation, and upon receiving my diploma, I physically saw the gap that distance learning created. Through no fault of anyone, I did not recognize most of the unit as many had left and were replaced. This also meant that very few knew anyone in my class, and we went many months without establishing professional connections. For many of us, this was probably overlooked as we were very disappointed to leave TRADOC. We survived a long time, and to verify the actual length of the course, a fellow peer had his first child right after graduation. It was, in fact, nine months.

One thing that I took advantage of was a piece of advice I took from a mentor in BOLC: "Nobody cares more about your career than you." When the pandemic occurred, there were a many hasty changes, and much of that impacted the students. Polygraphs were rescheduled, orders were delayed, and there were pay issues. It was understandable; a lot of departments started accommodating the new precautions to minimize the spread of the virus. As a lieutenant, I thought it was a great idea to email Human Resources Command directly and ask about orders, all during the middle of a pandemic and the height of the PCS season. I was very fortunate for who was at the receiving end, and I had my orders published by the following week for an assignment to the 915th Cyber Warfare Battalion. In hindsight, this was a great learning lesson. I acted well in advance to ensure I had time to prepare, and I communicated effectively to secure a desirable outcome.

Before I got to the 915th, I prepared by sending an introductory email with my resumé to the battalion commander. The welcoming response led me to believe this was a good call, and it broke the ice for the initial counseling. During the counseling, I brought up my interest to be a Cyber Planner for an Expeditionary CEMA (Cyber Electromagnetic Activities) Team (ECT). At the time, there was only one team, and that role was filled. However, the commander was receptive to my career goals and told me I will be on the list when the next slot opens. For the time being, I was placed into a developer role. Perhaps this would be my first broadening assignment since it was the opposite of a Cyber Planner.

In this role, I began the developer's Job Qualification Record (JQR). Every day, I tried to write legible code that compiled into an executable that met some criteria. If successful, the code was approved, and I would do this until I met each criterion of the JQR. Writing spaghetti code was already a hobby of mine, so it was a very rewarding position that helped me develop and learn more about programming.

My time as a developer only spanned six months, but it was rated time that made significant impacts. Since this was my first unit, I knew it was important to be resourceful and make a meaningful impression. I did that by assisting with several projects in conjunction with working on my JQR.

After six months, the team lead at the time for the ECT informed me that a Cyber Planner position opened and asked if I was still interested. I never met the team lead personally, but through some unforeseen networking, I came up on

the radar as a prospect. I transitioned to being a Cyber Planner, and up to now, it has been a very fulfilling position. Along with one other planner, I lead a group of intelligent Soldiers into a new frontier of cyberspace operations. The Cyber planner role was a very humbling position. I find myself reminiscing about CyBOLC when I learned I would be great at influencing people.

During my time with the team, I learned a lot about technical aspects; however, I learn more about the impact our leadership roles, especially in an emerging unit like the 915th. While the Army makes leaps and bounds to implement cyber operations, there is still the task of creating the awareness of cyber capabilities and providing a "so-what."

Last June, I attended a planning conference with a peer for the Multi-Domain Taskforce (MDTF) in preparation for Defender Pacific 21. We were tasked with briefing the MDTF (Multi-Domain Task Force) on 915th CWB capabilities. A half-hour before the brief, the organizer was going over the script with us, and he let us know it was okay to address the Cyber Center of Excellence Commanding General if there was further input. Much to my surprise, I inquired about the names of the attendees. The organizer responded: "there should be around 27 general officers present, including the MDTF and I Corps Commander." I learned to proofread, rehearse, and backwards plan in the thirty minutes leading up to that brief. The lesson I took away, however, was that the Cyber branch is still relatively new. There is a lot of information that we can and should provide as Cyber Officers to ensure we keep an open line of communication with the units we support.

I stayed an hour behind with my counterpart answering various questions on numerous cyber topics which proved to be very beneficial. This small amount of networking established many useful connections the 915th tapped when deployed to Guam for this exercise. Most of the MDTF staff were familiar with our team and were more than willing to help out in several instances. By the end, the 915th CWB built a vital relationship with the MDTF that will lead to future collaborations.

In summary, networking is undeniably a technical understanding Soldiers in the Cyber branch require. However, interpersonal networking is the skill that Cyber Officers need to continue improving in this organization. Whether it is for career goals or for the unit, there is something to gain with the appropriate amount and effective use of communication.

References:

Headquarters, Department of the Army. (2012, August). ADP 6-22 Army Leadership. HQDA.

GUAM -- Soldiers assigned to the 915th Cyber Warfare Battalion recently deployed to Guam with the Multi-Domain Task Force supporting Defender Pacific 21. According to 1st Lt. Kurtlynd McLane, a cyber planner with the 915 CWB Expeditionary Cyber Team, early involvement in planning conferences provided the MDTF and I Corps with insight on the 915th CWB capabilities and built a vital relationship with the MDTF that will lead to future collaborations.

Citizen Soldiers complete validation exercise to attain fully operational capability status

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade (Cyber)

HANOVER, Md. – U.S. ARMY NATIONAL GUARD SOLDIERS from four Cyber Protection Teams (CPT) completed their validation exercise (VALEX) in Maryland in July.

U.S. Cyber Command (USCYBERCOM) establishes the criteria for a CPT to attain Full Operational Capability (FOC), and the VALEX is an event the evaluators use to access the team's performance.

Two of the CPTs made up of personnel from Wisconsin, Illinois and Minnesota fall under the 123rd Cyber Protection Battalion currently mobilized as Task Force Echo V, and the remaining two are composed of members from California, Arkansas, Missouri and Nebraska.

The teams were evaluated by a Maryland CPT in accordance with criteria established by USCYBERCOM. The VALEX ensures the teams can meet the core training objectives and competencies required to be mission ready, said Maj. Brian Morgan, a team lead for one of the CPTs participating in the exercise.

"In order to be considered an operationally ready CPT, and part of U.S. Army Cyber Command's available forces, ready and prepared to support incident response, the team needs to be at FOC," said Morgan.

According to Lt. Col. David Garner, commander of the 123rd CPB and Task Force Echo V, said two teams were granted Initial Operating Capability status during TFE mobilization, and their next step was to pass the VALEX successfully. While engaged in the TFE mission, the team members worked after hours and on weekends to prepare for the exercise, he added.

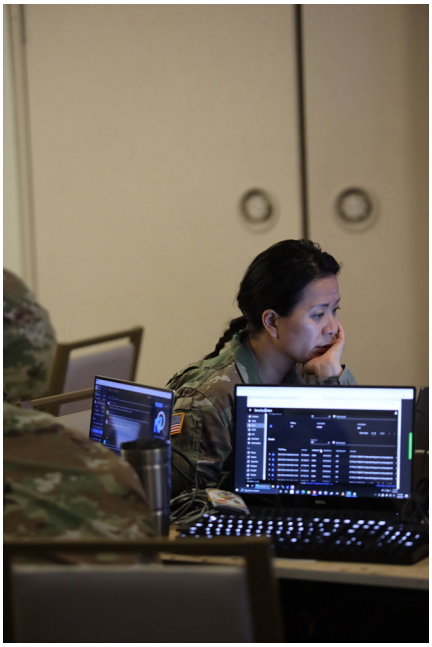
Now on its fifth iteration, TFE is comprised of Army National Guard Soldiers mobilized from the 91st Cyber Brigade to support USCYBERCOM operations full time, and is a testament to the Army's commitment to the Total Force in defense of networks against the nation's adversaries.

Garner praised the Soldiers flexibility and adaptability in preparing for the VALEX.

One of the CPT's cybersecurity operations officer and battle captain said citizen-soldiers have an advantage in being employed in cyber-related civilian careers, and also benefit greatly from partnering with their active-duty counterparts.

"The huge advantage we have is a lot of folks on the team are cybersecurity professionals and incident responders in their civilian careers. They do it for a diverse set of organizations, governmental, some private, some large, some small, so what you have is a wide variety of expertise," he said. "Additionally, we're working with very skilled, very professional Soldiers and Civilians, and getting the understanding on how they do things, some of the knowledge they have. We consume that knowledge, and we get to take it back to the state as a new set of experiences to enhance the capabilities that we have to improve our skills."Title 10 of the United States Code outlines the role of armed forces in the United States Code. It provides the legal basis for the roles, missions and organization of each of the services as well as the United States Department of Defense.

Since August 15, 2017, more than 600 U.S. Army National Guard Soldiers have been mobilized in support of Task Force Echo working alongside the 780th Military Intelligence Brigade (Cyber) to conduct cyberspace operations in support of USCYBERCOM and the Cyber National Mission Force. ■



Hanover, Md. – U.S. Army National Guard Soldiers from four Cyber Protection Teams (CPT) completed their validation exercise (VALEX) in Maryland in July. U.S. Cyber Command establishes the criteria for a CPT to attain Full Operational Capability and the VALEX is an event the evaluators use to access the team's performance...

The Honorable Order of Saint Isidore

THE HONORABLE ORDER OF SAINT ISIDORE recognizes individuals who demonstrate exceptional initiative, leadership, insight, and cyber excellence within their area of expertise. The award consists of the Gold, Silver and Bronze Medallion. The Gold Medallion recognizes individuals who have rendered conspicuous long-term service and significant contributions to the cyber mission force. The Silver is awarded to those who have contributions to the promotion of the cyber mission in ways that stand out in the eyes of the recipients, their superiors, subordinates, and peers. And the Bronze is given to those who have demonstrated the highest standards of integrity, moral character, professional competence, selflessness, while contributing to the betterment of the cyber mission force.

In April 2021, Armed Forces Communications and Electronics Association (AFCEA) considered and selected 16 of 30 candidates from 780th for the 2021 Saint Isidore Award. On behalf of COL Matt Lennox and CSM Ronald Krause, please join me in congratulating the following Praetorians.

Gold:
CW4 James Richards

Silver:
COL Benjamin Sangster
Christopher Rudy
MAJ Scott Beal

Bronze:
CW3 Jason OLafortune
CW3 Edison Rivas
CPT Alvaro Luna
Mr. Robert Ighnat
CW3 Scott Miller
SSG Brandee Lymon-Collins
CW3 Joseph Dixon
CPT Paul Baker
Mr. Aaron Tipton
1SG Stanley Collins
Jonah Cali
MAJ Stephen Hudak


MILITARY ORDER OF SAINT LOUIS

Cyberspace Developer's Course Critical to Retention and National Security

By Steven Stover, public affairs officer, 780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, Md. – Cyber Soldiers and a Marine graduated from the 11-month Tool Developer Qualification Course (TDQC) in a ceremony hosted by the 780th Military Intelligence Brigade (Cyber) at the Post Theater, July 13.

The United States Army has partnered with the University of Maryland Baltimore County (UMBC) to train Soldiers and Marines to become Cyberspace Capability Developers.

The nation's demand, makes the retention of cyberspace Soldiers more challenging; however, in addition to a unique mission set, programs like 170D, Cyber Capabilities Developer Technician (https://recruiting.army.mil/170d/) warrant officer recruitment; the 780th MI Brigade's in house certification of Network +; Security +; Certified Ethical Hacker and CISSP; and education partnership programs like TDQC are essential if the U.S. Army and Marine Corps want to retain the "best and the brightest."

Army Gen. Paul M. Nakasone, commander, U.S. Cyber Command and director, National Security Agency chief, Central Security Service, told the House Armed Forces Committee in March 2020, "I continue to pursue creative ways to leverage our nation's best and brightest to want to contribute to our missions."

According to the 780th MI Brigade S3 (operations) program managers, graduates of the TDQC course are proficient to an intermediate level in creating programs using the C and Python computer programming languages, and provides an education path for individuals to become experienced at 90 percent of the identified critical developer requirements that an individual must be able to articulate and demonstrate through practical application in order to be certified as a Cyberspace Capability Developer.

"Its purpose is to educate individuals who have little to no computer programming experience that have been identified through an assessment as having an aptitude and desire to become a computer programmer," said Sgt. 1st Class Corbin Greeff, a brigade senior Non-Commissioned Officer.

The 2021 TDQC graduating class includes: Spc. William Colley; Spc. Arthur Gould; Staff Sgt. Alex Jester; Sgt. Jerimiah Katen (distinguished honor graduate); Spc. Ewen MacGregor (honor graduate); Sgt. Michael Miano; Spc. Steven Mounie; Spc. Demetrius Nassy; Spc. Christopher Nguyen; Sgt. Jack Sanchez; Sgt. Steven Silbert; and Staff Sgt. Oliver Sung assigned to the 780th MI Brigade; and SSgt. Kotaro Fukasawa, Marine Corps Cyberspace Warfare.

Sgt. Katan, the distinguished honor graduate for TDQC Class 21-01, said the course gave him the tools that he needs to excel in his next position.

"I knew how to program o.k., before coming into the course," said Katan. "But for someone who is starting fresh it would be really beneficial because they go through a bottom-up approach and I believe it has prepared all of us, really well, to do our jobs."

Spc. Macgregor, the honor graduate for TDQC Class 21-01, echoed Katan's sentiments when he added, "TDQC taught us the basic building blocks of programming, a lot of the nuances for language base, like how to exactly do it or how to go about problem solving."

Katan and MacGregor, on behalf of TDQC class 21-01, wanted to express their sincere gratitude for all the UMBC faculty, with heartfelt appreciation to Liam Echlin and Dave Flanagan.

"They are probably two of the best instructors I've ever had," said Katan.

Maj. Micah Bushouse, the S3 (operations) officer for the 780th MI Brigade and guest speaker for the ceremony had these words of advice for the TDQC graduates.

"I am pleased to be among the first to congratulate you after nearly a year of academic work," said Bushouse. "More importantly though, I hope to someday meet the future you: a qualified cyberspace capability developer, who met the training certification requirements with enthusiasm honed by dedication; an experienced technical leader who enters the force; a lifelong learner who has walked the humble path; and an always curious researcher who is intolerant of ignorance and continually demands a deeper understanding. This future you IS what the Army (and Marine Corps) really needs, and you are the only person who can take steps today to get you there."

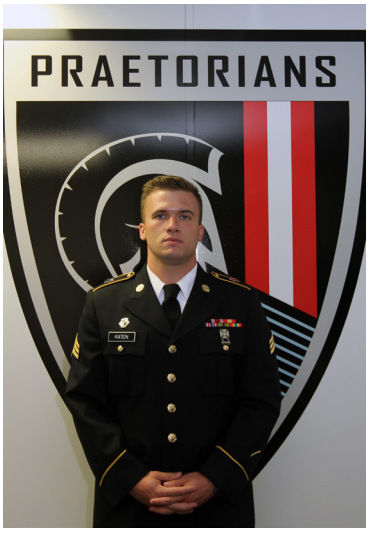
Congratulations to each of the 2021 TDQC graduates, and welcome to the world of capability development.

Since 2017, this is the eighth graduating class and with less than 100 graduates the selection process for applicants is very stringent. Soldiers interested in applying for TDQC should talk to their command team or contact the 780th MI Brigade S3 for more information.

How important is cybersecurity in the United States?

CyberSeek – an organization which provides information on the cybersecurity job market – shows a talent gap on their Heatmap (https://www.cyberseek.org/heatmap.html) of more than 460,000 job openings out of 1.42 million cybersecurity positions across the country, and with cyberattacks on the rise, the U.S. Bureau of Labor Statistics reports the demand for cybersecurity professionals is outpacing all other occupations and expects a 31 percent growth in the field from 2019 to 2029.

FORT GEORGE G. MEADE, Md. – Army Spc. Ewen MacGregor, a cyberspace operations specialist assigned to the 780th Military Intelligence Brigade (Cyber), was the honor graduate for the Tool Developer Qualification Course, an 11-month training program conducted in partnership with the University of Maryland Baltimore County to train Soldiers and Marines to become Cyberspace Capability Developers.

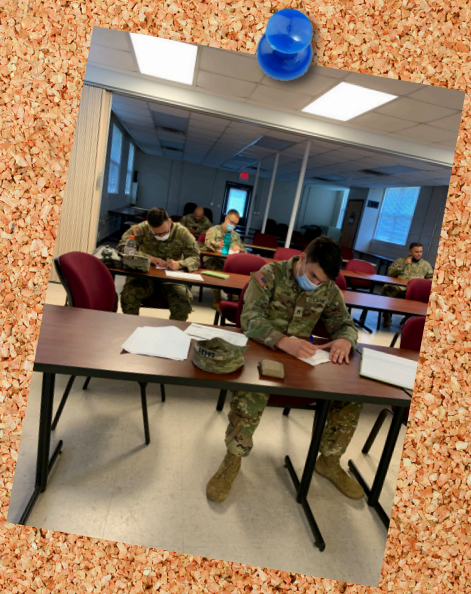


FORT GEORGE G. MEADE, Md. – Army Sgt. Jerimiah Katen, a cyberspace operations specialist assigned to the 780th Military Intelligence Brigade (Cyber), was the distinguished honor graduate for the Tool Developer Qualification Course, an 11-month training program conducted in partnership with the University of Maryland Baltimore County to train Soldiers and Marines to become Cyberspace Capability Developers.

FORT GEORGE G. MEADE, Md. – Cyber Soldiers and a Marine graduated from the 11-month Tool Developer Qualification Course (TDQC) in a ceremony hosted by the 780th Military Intelligence Brigade (Cyber) at the Post Theater, July 13. The United States Army has partnered with the University of Maryland Baltimore County (UMBC) to train Soldiers and Marines to become Cyberspace Capability Developers.

FORT GEORGE G. MEADE, Md. – Sgt. Wesley Smith, 780th Military Intelligence Brigade (Cyber), was presented with an Army Achievement Medal for attaining the Commandant's List after attending the Basic Leader Course, June 30.

FORT GORDON, Ga. – The 782d Military Intelligence Battalion (Cyber) is hosting ROTC Cadets this summer, and they began with their training with their sponsors and the Battalion Commander, July 19.



FORT GEORGE G. MEADE, Md. –Soldiers from the 915th Cyber Warfare Battalion began their quest to be recognized as the Best Warrior Soldier and Non-Commissioned Officer in a multi-day competition which includes a 12-mile ruck march, written exam, board and other Warrior-related tasks, August 2.

FORT GORDON, Ga. – 1st Lt. Conner Jarrio, a Cyberspace Operations Officer assigned to A Company (Cyber Archers), 782d Military Intelligence Battalion (Cyber), was promoted to captain and received his Oath from Maj. Rose Abido.

FORT GORDON, Ga. – Sgt. Megan Campbell, a Signals Intelligence Analyst assigned to A Company (Cyber Archers), 782d Military Intelligence Battalion (Cyber), was promoted to Staff Sergeant by her husband.

FORT GORDON, Ga. –
Sgt. Nicholas Polley, a Cyberspace Operations NCO assigned to A Company (Cyber Archers), 782d Military Intelligence Battalion (Cyber), was promoted to Staff Sergeant by Sgt. 1st Class (retired) Watkins.

FORT GORDON, Ga. – Soldiers from A Company (Cyber Archers), 782d Military Intelligence Battalion (Cyber), were promoted based on their potential for greater responsibility in a ceremony attended by their fellow Soldiers, Civilian teammates,

CAPERS ISLAND, s.c. – Charlie Company (Centurions), 782d Military Intelligence Battalion (Cyber), hosted a Warrior Adventure Quest event on Capers Island, South Carolina which included fishing, crabbing, hiking and a day at the beach, July 22. Soldiers and Family members from Alpha, Bravo, and Charlie companies attended and according to Capt. Jordan Salyer C Company commander “It was a great trip and a much-needed break for the Soldiers.”

FORT GEORGE G. MEADE, Md. – Christopher The Soldiers and Civilians of Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber), hosted a surprise celebration to congratulate Pvt. Kangni Lantchible on becoming a United States citizen.

FORT GEORGE G. MEADE, Md. – Christopher Helt, E Company, 782nd Military Intelligence Battalion (Cyber), receives the Joint Service Presentation pin from Gregory Platt, senior civilian advisor for the 780th MI Brigade (Cyber) in the brigade headquarters, August 17.

FORT GEORGE G. MEADE, Md. – John Francis, Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber), receives the Meritorious Civilian Service Medal from Lt. Col. Jesse Sandefer, the brigade deputy commander, July 1.

FORT GEORGE G. MEADE, Md. – Chief Warrant Officer 2 Barry Mitchell, Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber), receives the Army Achievement Medal from Capt. Lauren Feifer, the HHC commander, July 1.

FORT GEORGE G. MEADE, Md. – Chaplain (Col.) Suk Kim, the Fort Meade Senior Garrison Chaplain, was the guest speaker for this month's Brigade Resiliency Talk Luncheon in the Brigade Annex, September 1. Kim talked about what you are filling you cup with, that we're going to make mistakes, we're not perfect, but to not quit. He used the Army acronym PMCS (Preventive Maintenance Checks and Services) as a technique we can use on ourselves. If you require support, the 780th Military Intelligence Brigade Unit Ministry Team can be reached at: usarmy.meade.780-mi-bde.mbx.unit-ministry-team@mail.mil.

FORT GEORGE G. MEADE, Md. – Soldiers, Army Civilians, and their Family members participated in a warrant officer promotion ceremony hosted by the 781st Military Intelligence Battalion (Cyber), whereby Chief Warrant Officer 2 Christopher Shepard was promoted to CW3 (left), and Warrant Officers Gordon "Stu" Philips (center) and Richard Soto (right) were promoted to CW2, September 10 on the Fort Meade Parade Field.

NEXT QUARTER'S BYTE IS focused on the 780th Military Intelligence Brigade's tenth anniversary. In December 2010, the Army approved the establishment of a cyberspace operations brigade, and one year later, on December 1, 2011, the 780th MI Brigade officially unfurled its colors for the first time during a ceremony at Fort Meade, Maryland. If you have an article to share, write a synopsis paragraph and send it to Steven Stover at steven.p.stover.civ@mail.mil NLT Oct. 15, 2021. Articles are due Nov. 1, 2021.

Save the Date!

AvengerCon VI is returning on

November 29th and 30th!

AVENGER CON