780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 11, Issue 3

INNOVATION:
Breaking Paradigms

780th MI BDE
"STRENGTH AND HONOR"

COL Benjamin Sangster
Commander
CSM Jesse Potter
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@army.mil, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.

On the Cover

SCHOFIELD BARRACKS, Hawaii – SSG Ryan Hedgcoth, expeditionary CEMA operator, ECT-01, carries a TRAC (Tactical RF Applications Chassis), platform that enables mission tailored, CEMA capability deployment through soldier interchangeable payload cards, radioheads, and antennas for RF band-specific applications. The system allows for various CMOSS (Command, Control, Communications, Computers, Intelligence, Reconnaissance, (C5ISR)/Electronic Warfare Modular Open Suite of Standards) compliant cards to interact with the electromagnetic spectrum, March 30.

BACK IN MARCH, COL BEN SANGSTER, PRAETORIAN 6, commander of the 780th Military Intelligence Brigade (Cyber), stated his intent for this edition of The BYTE Magazine to focus on innovation.

He provided his guidance to the battalion commanders, while observing the 11th Cyber Battalion Operational Readiness Assessment (ORA) at Schofield Barracks, Hawaii, when he told them "Think capabilities, tradecraft, talent management – whatever you can apply the concept of innovation to as it applies to our formation and community."

According to LTC Benjamin Klimkowski, former commander, 11th Cyber Battalion, while tradecraft and partnerships were important throughout the ORA, it was the Soldier's innovation that was critical to mission success (story on page 21).

"We are breaking paradigms here where we are not getting a fielded, complete system with a tight training circular, and a tight understanding of what this system does," said Klimkowski. "We have smart analysts, operators, and developers working together to extend the capabilities and use them in ways that are very powerful. Our Soldiers make it look easy, but it is not normal; the 11th Cyber Battalion has a unique mission and culture where incredible talent like what you see here can flourish. It's really the technicians with the expertise and initiative that are refining and extending capabilities– not just employing– and using existing technologies in ways that were not initially envisioned."

Also, in this edition, we pay our respects to SGT Ammel Rhyes M. Dooley, B Company, 782d Military Intelligence Battalion. A memorial service for SGT Dooley was held on April 28 at Fort Eisenhower, GA. His passing affected a great number of Soldiers and Civilians and their Family members. He will be remembered and missed.

Praetorians! Strength and Honor

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

Innovation

THROUGHOUT HISTORY, INNOVATION HAS PLAYED A KEY ROLE in deciding who was victorious in war…and who was not. The advent of the rifled musket in the 18th and 19th century added both power and accuracy to the infantrymen. Braking systems on field artillery pieces around the turn of the 20th century advanced indirect fires, decreasing the amount of time it took to re-aim an artillery piece after it was fired (due to the recoil moving it off target). Barbed wire was invented towards the end of the 19th century and played a critical role in the trench warfare of World War I. The invention of the radio in 1901 was a game changer in modernizing command and control during war. In World War II, Alan Turing's invention of a machine known as the Bombe was critical in efficiently decoding the German's Enigma code enabling the allies to decode German communications. Twentieth century inventions such as nuclear weapons, GPS, and stealth aircraft have turned world powers into global superpowers.

Historically, it was which side was able to innovate that made the difference. Today, innovation alone is not the deciding factor in who wins, or who loses. Without innovation, you will lose. With innovation, at best, you will keep pace with your adversary. If you want to win, you have to be able to innovate faster than your adversary can.

Looking back at the previously mentioned examples of innovation, the timescale was measured in months… maybe even years. The cyber war that we are engaged in, today…the timescale for the innovation necessary to keep pace with our adversaries is measured in days, at best. Between 0-day and N-day vulnerabilities, adversaries have a menu of options that they can customize to gain access and achieve their desired end state. Whether that is intellectual property theft or D4 (deny, degrade, disrupt, destroy) of critical systems, our adversaries continue to leverage security flaws to forward their agenda. Our Cyber Operators and Analysts must move (at least) as quickly as our adversaries to shore up our defenses, as well as, take advantage of the same vulnerabilities so we are positioned to persistently engage our adversaries at the time and place of our choosing.

When you think about innovation, especially in the cyber domain, the first thing you probably think of is new technology (hardware or software) that changes or improves the way we do something. Take the mobile phone, for example. I remember when my parents purchased their first "mobile" phone. It was the Motorola Bag Phone. I can't remember how it was powered, but can only assume it plugged into the cigarette lighter. Regardless of how big and cumbersome it was, we definitely could make telephone calls from the car. The reliability and quality of those calls was questionable, at best. I'm sure my family iterated through multiple versions of mobile phones. I remember my first mobile phone when I was a lieutenant. Wasn't anything fancy, but it definitely was more reliable than my parent's bag phone. Along came the Blackberry, and eventually the iPhone. Fast forward to today. We hold more compute power in our hands than any computer available to the public dating back to around the turn of the century.

Innovation cannot be limited to just technology. We must ensure that we are innovating our talent management programs, our doctrine, and many other non-technologically based systems. The theme for this edition of The BYTE is innovation. I hope you enjoy the articles we have delivered. As long as one of those articles causes you to intellectually engage the concept of innovation, making you think about how you or your team can out innovate the adversary, I will consider it mission accomplished.
Everywhere and Always in the Fight! Go Tigers!

-Praetorian Six

SCHOFIELD BARRACKS, Hawaii – Maj. Gen. Neil S. Hersey, Deputy Commanding General – Operations for U.S. Army Cyber Command, was present to observe Soldiers from the 11th Cyber Battalion, 780th Military Intelligence Brigade (Cyber), refine tactical Cyber-Electromagnetic Activities (CEMA) concepts for the Army during an Operational Readiness Assessment here in late March 2023.

Task Forces vs. Teams: Differences in Operational Approaches for OCO

By LTC Donald Sedivy, Commander, 781st MI Battalion, Vanguard

WITH THE EVER INCREASING DEMAND for offensive cyberspace operations (OCO), optimizing existing resources to maximize operational output is of keen interest in a zero-growth environment. In 2012, the Joint Staff and U.S. Cyber Command direct establishment of 133 Cyber Mission Force (CMF) teams to execute CYBERCOM's mission to direct, synchronize, and coordinate cyberspace operations in defense of the nation. Since that time, CMF teams have been the fundamental unit of action for both offensive and defensive operations. The Cyber National Mission Force (CNMF), originally activated in January 2014, started with 21 teams, 13 Cyber National Mission Team (NMTs) and eight National Support Teams (NSTs). At present, the CNMF has 39 joint cyber teams under its command. While ADP 5-0 does not specify a hard limit for what a feasible span of control constitutes, it does note that "increasing the number of subordinate units increases the number of decisions that a commander must make, and that may decrease agility". A span of control of 39 under a single headquarters does not promote the agility required to execute of cyberspace operations at pace with our adversaries. In response, by organizing its 39 teams into six task forces (TFs), the CNMF is executing operations in a manner that imposes a more feasible span of control over its elements while allowing for efficiencies of scales for low-density, critical functions.

Overview of Team-Centric Operational Model

To gain appreciation for the advantages and disadvantages of organizing into task forces, it is useful to examine the original team-centric model for OCO. As indicated in Figure 1, a 58-person NMT is organized into three primary types of elements: a support element, an intelligence element, and five mission elements. The primary purpose of the support element, which contains the team leadership, is to generate plans and identify targets derived from their higher headquarters orders and guidance. Those initial plans and targets are then passed to the intelligence element to conduct additional analysis and reporting based on access to SIGINT as well as incorporating any relevant all-source information. If gaps exist in data available within the SIGINT system, the intelligence element can task the team's mission elements with requirements specified in a collection plan. Those mission elements then conduct cyberspace operations under the appropriate authorities to collect mission data and artifacts which are then passed back to the intelligence element for additional analysis and reporting. This cycle continues until the support element confirms that the appropriate intelligence and supporting information has been generated to submit a mission package. Once a mission package has been approved by a higher headquarters, that package is then passed to a mission element to execute effects, typically enabled by tools built by cyberspace capability developers. The advantage of the team model is that all of authorities and expertise to generate the intelligence to support cyberspace operations as well as to execute those operations is under a single C2 structure. CMTs have the same structure and work roles as NMTs but different requirement for work role proficiency based on CYBERCOM requirements. NSTs, as depicted in Figure 2, and CSTs operate under a similar construct. However, since NSTs and CSTs do not contain mission elements, they conduct intelligence operations in support of NMTs and CMTs respectively (as implied in the word "support" in NST and CST).

Overview of TF-Centric Operational Model

The basic premise of a CNMF Task Force (TF) (recently designated Joint Task Forces (JTFs) on April 10, 2023) is to consolidate planning and mission command functions under a single commander with a support staff that has multiple Joint Mission Teams (JMTs) and an operations element task organized under it. CNMF JTFs are comprised of CNMF-HQ billets, NMTs, NSTs, and National Cyber Protection Teams (N-CPTs) that are task organized with the minimum authorized structure depicted in Figure 3 as starting point but uniquely configured based on their mission requirements. The task force staff generates plans and identifies targets based on CNMF orders and guidance in a similar manner to a support element for a team, but on a larger problem set. The JMT is an evolving construct that is typically modelled after the team intelligence element augmented with an exploitation analyst (EA) but can also contain DCO mission elements and other maneuver forces at the discretion of JTF CDR. JMTs are also typically task organized to include members from multiple services rather than being service pure constructs as NMTs / NSTs / N-CPTs are presented to the Joint Force. The JMTs receive initial plans and targets from their JTF staff that they then conduct additional analysis and reporting in a similar manner to a NMT or NST intelligence element. The operations element consolidates a pool of operators and EAs from multiple teams into a single element that is tasked by JMTs and JTF leadership to conduct operations in a similar manner that team mission elements would do in support of its intelligence and support elements.

Compare / Contrast of Operational Models

The most obvious and biggest advantage of TF over the team model is one of scale. A single team can only generate enough intelligence to support a limited number of targets with the fixed overhead of its support element in a 1:1 ratio. In the TF construct, support element functions are consolidated into a staff that has advantage of pulling their resourcing from multiple teams. This means that TF staff functions can be built more robustly and with more redundancy in critical low-density work roles (fires planner, linguists, and reporters) than their team counterparts. This enables them to support multiple intelligence elements (JMTs) simultaneously while being able to identify when efforts are either duplicative or reinforcing and address appropriately. Additionally, the number of targets that a TF staff can support scales linearly with the number of NMTs and NSTs that it supports. Specific to CNMF, TFs also solve the span of control problem that affects it agility by decreasing its span of control form 1:39 down to 1:6. With respect to mission elements, consolidating operators at the TF level allows the different specializations for operations to be dynamically organized based on mission requirements ensuring that their skills sets are always in use rather than having to have all specializations that a team might require maintained on each team regardless if there is a current requirement. Lastly, by task organizing across services within TFs, each service has the opportunity to compensate for shortfalls that may exist with a different service's manning or training construct.

While there are many benefits to the TF construct, there are some additional considerations and potential disadvantages to this implementation. Firstly, investing in the creation TF staffs out of CMF teams assumes that the mission alignment of those teams is likely to remain consistent. Changing the alignment of teams that source TF staff positions would be highly disruptive to a TF and affect its ability to provide operational support if it were to occur on a routine basis. Teams are stand-alone units that can be dynamically task-organized under different headquarters with little difficulty. Additionally, task organizing JMTs across services creates potential friction as there will be a bifurcation between who is responsible for administrative support versus operational direction. Managing this arrangement requires constant messaging and reinforcement from both TF leadership and supporting service commands to ensure all requirements are met.

Conclusion

With the need to drive and conduct cyberspace operations with an agility that can keep pace with our adversaries, the CNMF's decision to operate as TFs greatly reduces its span of control to accomplish its mission. A TF-centric operational model also reduces the fixed overhead of support staff found at the team level while allowing for more robust and scalable staff support to enable its subordinate elements to generate the intelligence support to as well as execute cyberspace operations. Teams are more readily task-organized to different headquarters and can be effective as long as the headquarters above them has the appropriate span of control to support them effectively.

References:

[1]https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/#:~:text=CMF%20teams%20execute%20the%20command's,and%20accomplish%20their%20assigned%20missions

[2]https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe/

[3]Ibid

[4]ADP 5-0, Paragraph 2-21, dated 31 July 2019

[5]https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cybe/

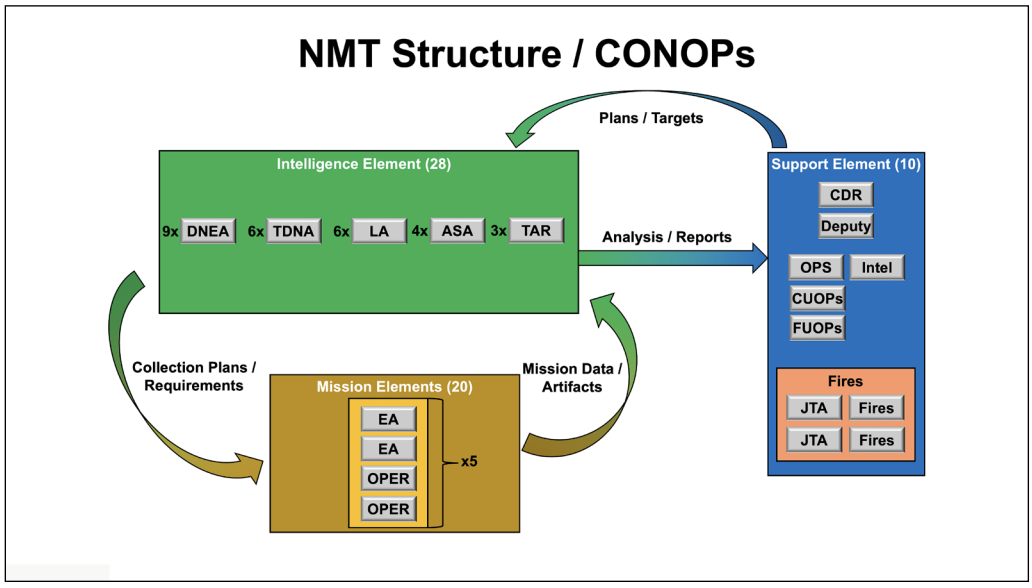


Figure 1. NMT Structure / CONOPs

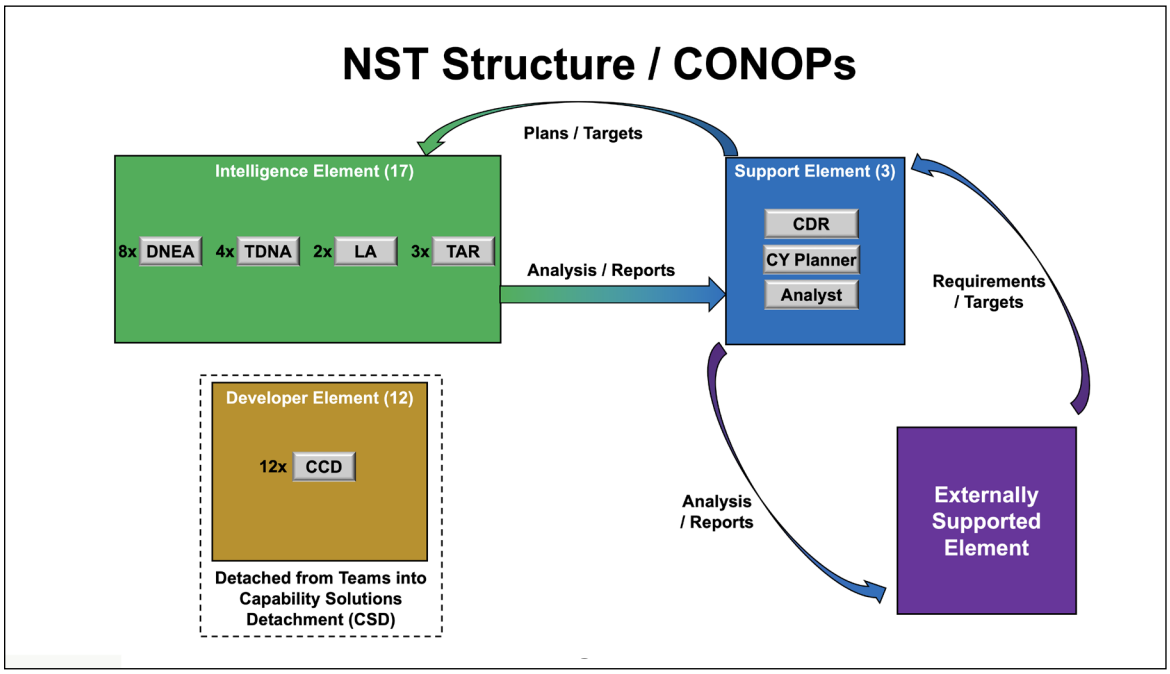


Figure 2. NST Structure / CONOPs

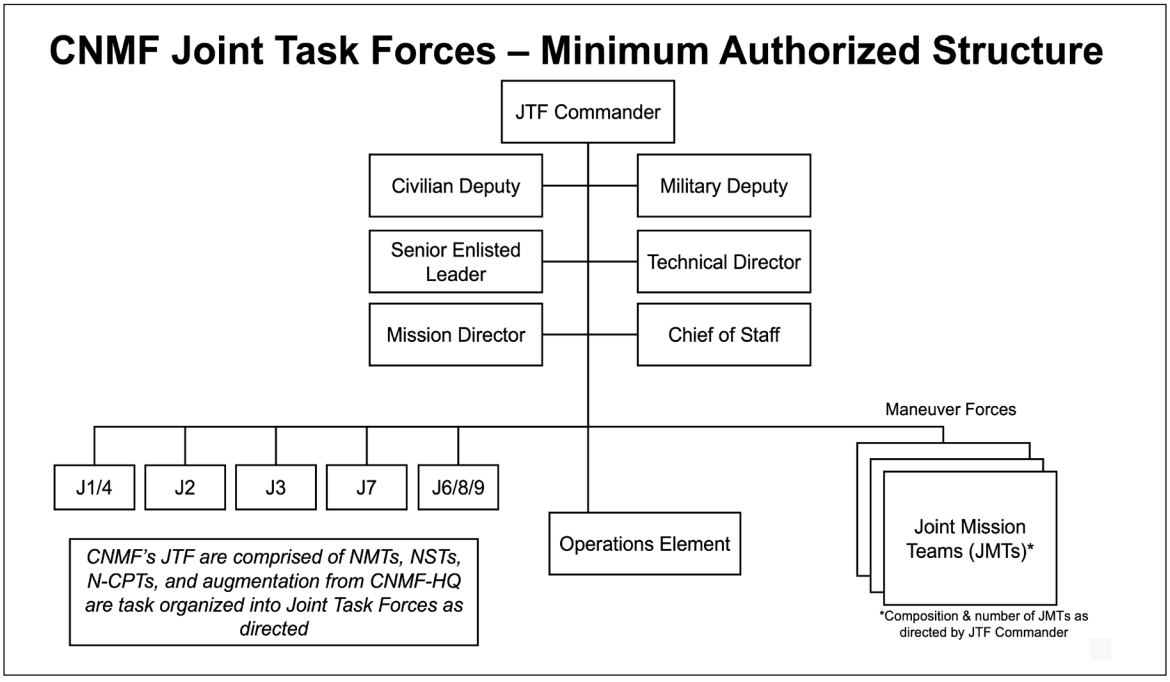


Figure 3. CNMF Joint Task Forces - Minimum Authorized Structure

Tradecraft Academy: Partnering to Build Advanced Skill Proficiency

By LTC Donald Sedivy, Commander, 781st MI Battalion, Vanguard

AS CYBER MISSION FORCES CONTINUE TO EVOLVE the scope and sophistication of their operations, the demand for advanced levels of proficiency across all work roles has increased to meet U.S. Cyber Command's readiness standards. Such levels of proficiency require dedicated time and expert knowledge to generate which come at the cost of time dedicated to operations. However, if the time isn't invested in training then the speed and quality of operations suffers. By investing time from subject matter experts to create a standard set of products in partnership with a Joint Task Force, 781st has demonstrated feasibility of executing a one-week academy for advancing experienced analysts in the Digital Network Exploitation Analyst (DNEA) and Target Digital Network Analyst (TDNA) work roles from basic to senior analyst proficiency in a time condensed manner. This "Tradecraft Academy" model demonstrates an effective approach where the supporting service command (colloquially referred to as the "ADCON" command) and the supported operational command ("OPCON" command) work together to achieve an increased force readiness posture.

Overview of Tradecraft Academy

The premise of Tradecraft Academy is to identify the various components of the DNEA and TDNA senior JQRs that are suitable to be presented into condensed blocks of instruction. Upon completing all blocks of instruction, individuals would be afforded an opportunity to demonstrate that they had retained and could apply their knowledge. Conducting a cross-walk of task suitability for instructional blocks, B Company, 781st discovered approximately 90 percent of Senior DNEA and 80 percent of Senior TDNA Module 3 individual line items fall within this category as indicated in Figure 1. For the pilot iteration of Tradecraft Academy, B / 781st created instructional content to cover approximately 70 percent of Senior DNEA and 66 percent of Senior TDNA line items as also indicated in Figure 1. Mapped in time, to generate the content it took 10 instructors approximately six hours spread over two months to create two to four hour blocks of instruction with an additional three instructors taking approximately 10 hours spread over the same two month period to create a five to seven hour blocks of instruction and discussion. To manage the preparation and execution of the event, the OIC and NCOIC for the academy spent approximately 60 hours over a three month period. The execution of the event required three days of work role agnostic training (enabled by the overlap of DNEA and TDNA line items), one day of work role specific training for DNEAs and TDNAs, and one day of JQR testing and line items sign offs. Training sessions were conducted through a combination of Skype video calls over NSANet and in-person sessions in SCIF spaces.

While B / 781st was able to create the material by leveraging senior and master qualified individuals within their company, having the protected time to execute the training with a wide enough audience to make the effort worthwhile required approaching their supported task force (TF) commander to have a week dedicated to training. The TF CDR was able to select a week, forecasted approximately one quarter out from execution that minimized the impact to operational efforts. Additionally, coordinating with the TF CDR provided the visibility to the other services within the TF who were also interested in the Tradecraft Academy resulting in increased participated as well as future availability of additional instructor support.

The pilot iteration of Tradecraft Academy was executed from March 20-24, 2023 with target audiences of 15 DNEAs and eight TDNAs. The average analyst completion of DNEA Module 3 line items was 45 percent with one individual completing 100 percent of their senior DNEA JQR during the week as indicated in Figure 1. The average analyst completion of TDNA Module 3 line items was approximately 20 percent with one individual completing 100 percent of their Senior TDNA line items as also indicated in Figure 1. The primary limiting factor for line item completion during the pilot iteration was the ratio of senior DNEAs and TDNAs to senior aspirants to facilitate line item sign offs.

Benefits of the Model and Lessons Learned

The four primary benefits of the Tradecraft Academy are predictability for the operational command, flexibility with slotting when multiple Tradecraft Academies are conducted, protected time for senior aspirants to complete their line items, and scalability. With regard to predictability, coordinating with the operational headquarters three months prior to execution created the appropriate amount of standoff from current operations to ensure the training time nested with its operational cycle to prevent the loss of momentum on any efforts. For flexibility, if multiple iterations are conducted across different TFs, each TF has the ability to slot individuals in another TFs iteration. This occurred during the pilot iteration where a sister TF needed a senior TDNA to be certified which B / 781st was able to facilitate. In regards to protected time, since most analysts performing at the senior level often serve additional roles within their TF, having a week exercise gives the protected time for both high performing basics to attend the training and experienced senior analysts to execute the training. For scalability, with the content now

generated, executing successive iterations only requires 30 hours of coordination for two effort leads and seven hours per instructor to review, rehearse, and execute the training for 10-13 instructors. In terms of lessons learned, based on the results of the pilot iteration, it is recommended to have an additional day for testing and line-item sign offs if additional evaluators are unavailable for a single day. Moreover, to ensure analyst that complete the Tradecraft Academy actually complete all of the sign offs senior aspirants are eligible for, first-line supervisor engagement and back briefs on progress are recommended.

Conclusion

To achieve advanced levels of work-role proficiency, partnership between supporting service commands and supported operational commands is required for an efficient and effective execution. Tradecraft Academy represents one such approach focused on the DNEA and TDNA populations for the Cyber National Mission Force (CNMF). As of June 2023, Tradecraft Academy is currently in staffing for implementation across the CNMF and its model is easily exportable to other commands.

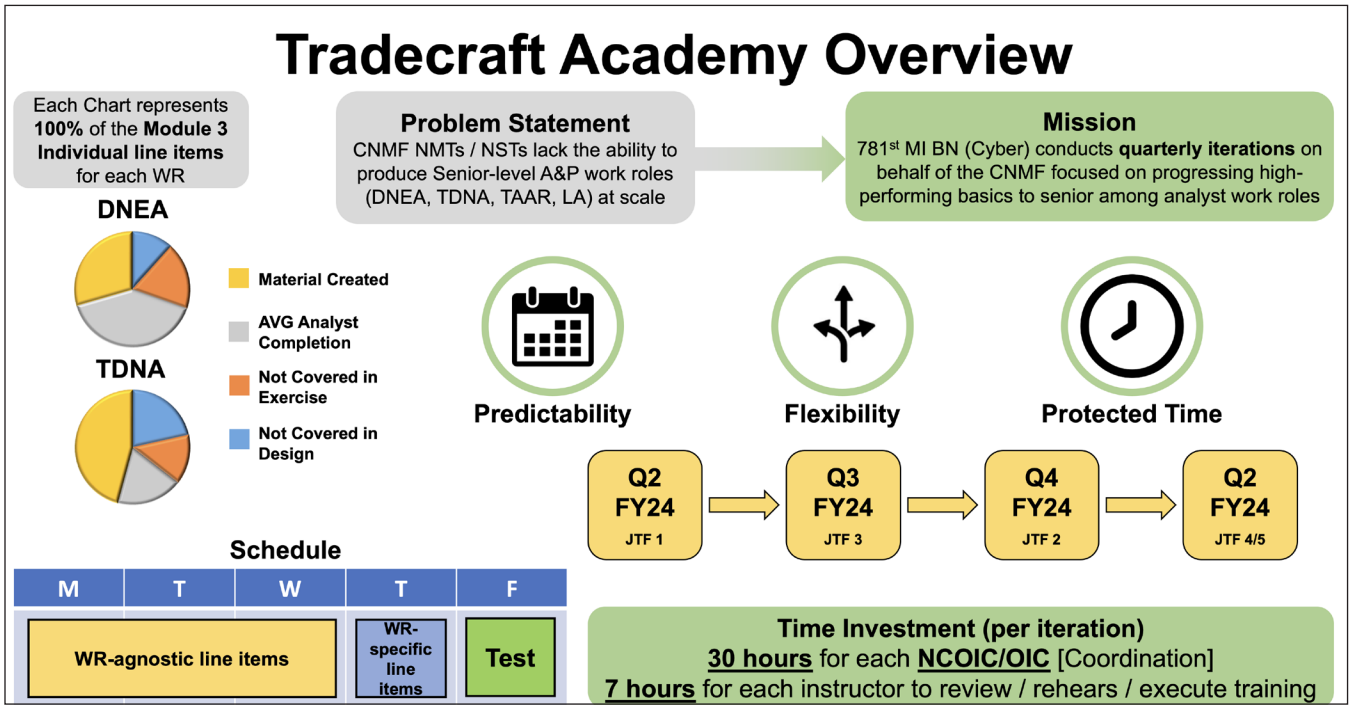


Figure 1. Tradecraft Academy Overview

Empowering People and Organizations through Workflow Automation

By CPT Joshua Fielder, Commander, Charlie Company, 782d MI BN (Cyber)

Invest in People

At every echelon, U.S. Army Commissioned Officers are investing in people, striving to accomplish the team's mission, and inspiring organizations to reach their full potential. There are many ways to for Officers to invest in people: by knowing our people and the organization, by ensuring their well-being, by rewarding their achievements, by believing in their potential, and by creating a supportive work environment to help them to succeed. Ultimately, we invest in our people because every person has intrinsic value and is worth the investment of our time and our energy. Officers care about their people's work because we are a team, rallied around a common purpose, which is our mission.

Achieve the Mission

Officers achieve their mission by investing in people. As a Brigade, our operational mission is to conduct Offensive Cyber Operations to deliver effects in support of Service Cyber Components (Army Cyber, Air Force Cyber, etc.) and Joint Force requirements. One could argue that the mission is simply "to give some really bad guys some really bad days" but arguing semantics is outside the scope of this article. Our Brigade's administrative mission is to ensure teams are manned, trained, and equipped in order to effectively conduct operations. But as Commissioned Officers, our mission is foremost to invest in our people. The care of our people is the proverbial center of gravity; caring for people is how we achieve the Brigade's operational and administrative missions because without our people we cannot achieve the mission

Modernization as an Enabler

The U.S. Army has provided invested in analytic and intelligent services to assist Officers in achieving their mission of caring for the health and welfare of their Soldiers. The Commander's Risk Reduction Toolkit (CRRT) provides a comprehensive report on each Soldier's administrative records, assignment history, medical data, and more. Integrated Personnel and Pay System – Army (IPPS-A) is a platform used to manage duty assignments, promotions, requests for pay, absences, among many other features. Microsoft 365, as a unified suite of platforms, enables teams to share data and collaborate on projects.

In an effort to create a unified environment for analyzing readiness, many of these platforms import data from multiple Army enterprise systems. In CRRT, a data analytics platform, we can even explore the data lineage to see how information is ingested into the platform.

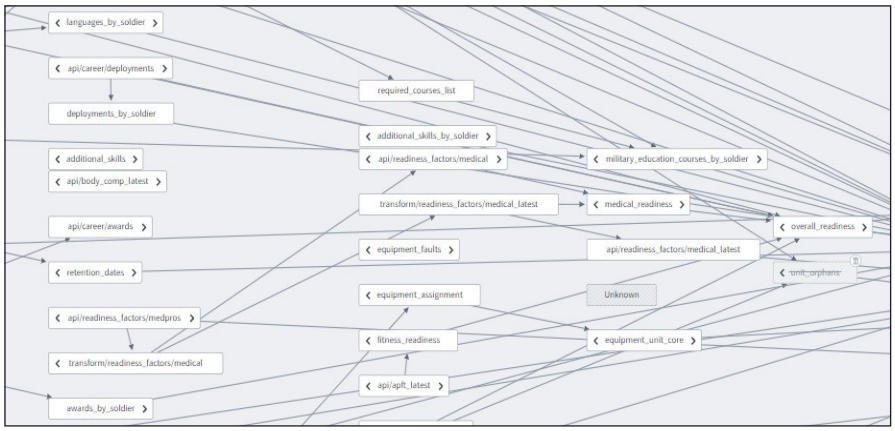


Figure 1. Excerpt of Data Lineage from CRRT

With an amalgamation of innovative platforms, leaders are challenged to learn and integrate new procedures for analyzing data and generating reports. Depending on the application, the procedure for generating reports is often built on object-oriented programming where the user can drag and drop a function to manipulate the display of information. In other cases, a bespoke solution using custom coding is needed to perform an action.

Officers invest in people by using these platforms to their advantage. The platform (or services) of Microsoft 365 is being used in many circumstances to support the care and welfare of our people. Battalion staff use this platform for tracking the status of Requests for Orders (RFO). And at the Company-level, Commanders are using it to track and disseminate training and readiness requirements down to the individual Soldier. Many of the platforms have the ability to invest in our people by executing tasks at speed and with accuracy using the feature of workflow automation.

Workflows

Let's start with the basics: what is a workflow? A workflow is a collection of tasks (or actions) that are performed in a specific order. To give an Army example of a workflow: Plan, Brief, Execute, Debrief (PBED) consists of four actions performed in a specific order. We use workflows to ensure that a series of tasks are executed in the correct order, with speed and accuracy. Once the workflow begins, each action is expected to be performed in sequence, step-by-step.

Automation

Next, let's take a look at automation of workflows and why automation is an advantageous feature. A complex workflow may include logical statements (if this circumstance is true, then perform an action) or rules to create

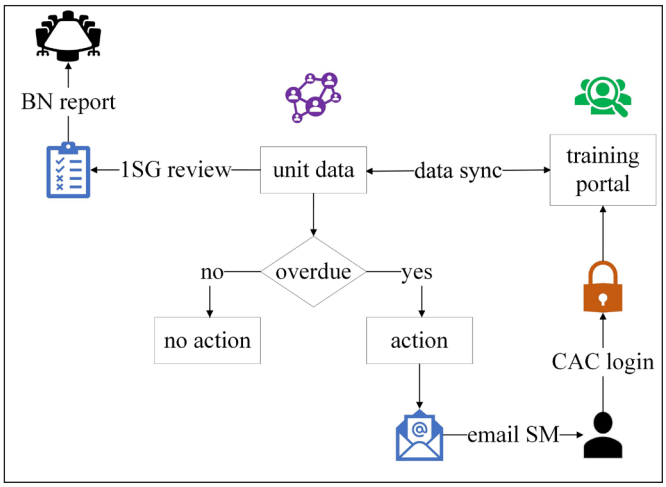


Figure 2 – Workflow diagram using Microsoft 365's suite of online services. Unit readiness data is stored in MS Lists, MS Power Automate analyzes overdue readiness requirements, notification of overdue readiness is sent through MS Outlook, personnel are added into the unit with group management in MS Teams, the training portal is hosted on MS SharePoint, and readiness metrics are calculated using MS Power BI to inform BN reports.

unique actions or to modify the flow of information. Workflows could be performed manually, requiring someone to step through every action in the sequence. But what if that workflow has to be repeated for each SM in a unit? For example, a workflow could be analyzing annual training and readiness requirements for each SM in a unit, with 30+ requirements and 70+ SM, that's over 2,000 dates that would need to be reviewed. If we wanted to also determine who is approaching the annual requirement, or who is missing completion dates, and we do these reviews on a regular basis, the process becomes exponentially difficult to perform manually. Automation helps to negate the need for manual effort by defining a set of rules or logic that allows the workflow to autonomously execute a series of actions.

To get started with caring for people with workflow automation, Officers identify task(s) that need to be automated and which platform is most suitable to perform the automation. For example, when COL Sangster took command of 780th MI BDE (Cyber), he identified a need to improve the Cyber Assignment Incentive Pay (CAIP) workflow. He provided his intent to improve the flow of communication, the accuracy of forms submitted by companies, and the speed of processing CAIP requests from the SM through the BDE. With his intent a platform was identified to automate the process of submitting requests for CAIP. So the BDE Deputy Commander, a team of developers, and BDE staff among others worked together to creatively implement a solution using Microsoft 365's suite of applications along with a custom web application that communicated with a server. They used automation to process the SM's information and cross-reference current ARCYBER guidance to pre-fill a series of PDF forms that were required to request CAIP. They also used automation to send email notifications as packets moved through the workflow and integrated a status tracker into a support channel on MS Teams to track and comment on the status of requests.

After creating an automated workflow, it is a best practice to test the automation with sample data before fully implementing the solution in a live, production environment. There are instances where coding-on-the-fly may be necessary, but it's important to avoid accidentally spamming your entire organization when testing automation features. After a flow's execution, it is also important to review the results and monitor future executions of the workflow to ensure it continues to operate as expected

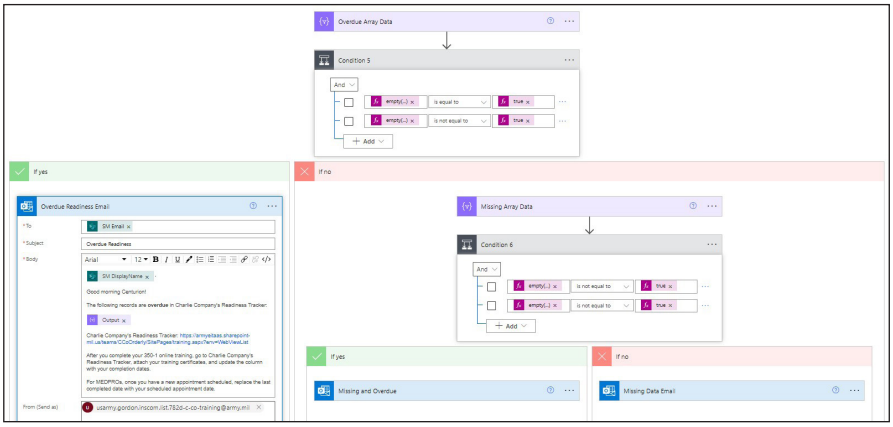


Figure 3 – Exert of an automated workflow from Microsoft's Power Automate; this flow automatically sends bi-weekly readiness notification emails tailored to the SM. Using the workflow from Fiture 2, when a SM completes their annual trianing requirement, they enter the completion date in the training and readiness portal and will not receive another reminder for that training event until they are approaching 365 days following the completion date.

Empowering People through Automation

Appeal: Officers invest in people by using automation to empower staff to do tasks that are more appealing, creative, and less repetitive. Reporting on large datasets can be mundane and repetitive work. When staff are able to pass the toil of repetitive tasks to automated workflows, they are free to focus their attention on creative tasks and increase the unit's productivity. Doing repetitive tasks can be time-consuming, taking people away from projects that allow us to use our creativity. When we save time with automation of repetitive tasks, we can refocus our attention on other projects like creating a positive and enjoyable work environment.

Awareness: Automation empowers SMs to gain visibility over highly accurate data and the potential (given permissions) to modify or interact with their data. Referencing Figure 2, automating notifications of annual training and readiness requirements has been used to empower SMs. The workflow consists of a series of actions: querying a company-level database, analyzing a SM's data for deficiencies, compiling a report on each readiness requirement, and concludes by notifying SMs with a detailed report on which requirements are currently soon-to-be overdue. The SM now has visibility of their requirements and access to resources to take care of their training requirements.

Alerts: With automated email notifications of overdue readiness requirements, SMs are reminded of annual training and readiness requirements in the frequency defined by the leader's preference. Within the email, the SM receives a link to the company's Training and Readiness Portal where they can use a CAC to securely login. In the training portal, the SM may only view their information; each person's data is protected by access control allow lists. Next to the training and readiness requirements are links to access requisite training and contact information to schedule appointments for medical or records deficiencies. By updating their information in the portal, the SM will no longer receive a notice of that deficiency in subsequent email notifications.

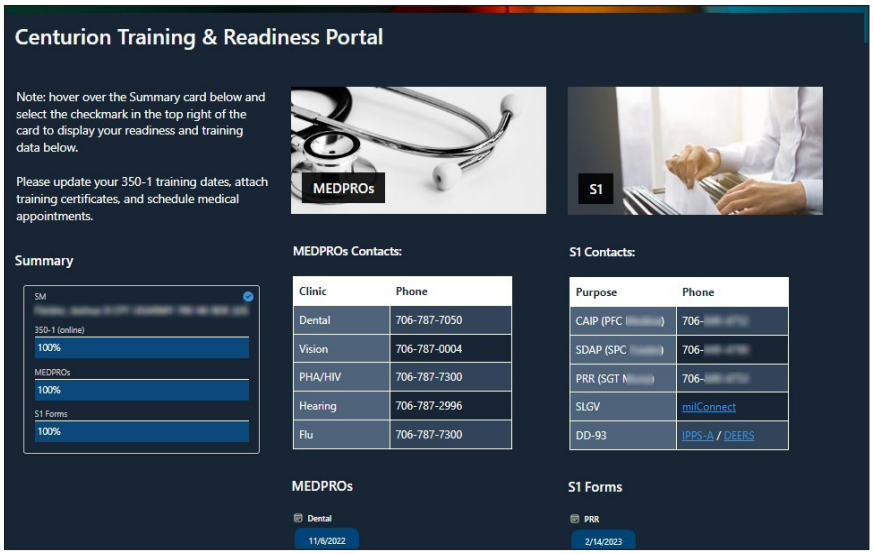


Figure 4 – Charlie Company's Training and Readiness Portal. After securely logging into the portal via CAC, the SM's can access training links, upload training certificates, and update their completion dates.

Opportunities for Future Automated Workflow Projects

The potential applications of workflow automation are only limited by our imagination. Broadly speaking, some of the future uses of automation could include:

- Individual development; providing Soldiers with personalized training plans.
- Operational employment; using events as triggers to execute effects.
- Situational awareness; monitoring forums for zero-day exploits relevant to our targets.
- Digital Wellness; surveying our calendars for opportunities to schedule a break from looking at a computer screen and possibly take a short walk to improve our health.
- Improving efficiency; turning manual, repetitive tasks into scheduled events.
- Recognizing performance; notifying recommenders of upcoming suspenses to draft PCS / ETS awards.

There are even platforms that already have the potential to benefit Offensive Cyber Operations with automation of workflows that may not be currently used in their full potential: the Army's Big Data Platform (BDP) applications and Joint Cyber Command and Control – Readiness (JCC2-R) are the first two platforms that come to mind. Commissioned Officers will continue to conjure up creative approaches to use innovative technologies for the purpose of investing in our people. We value people and care about their health, safety, development, and success; efficiency and productivity are simply the welcomed byproducts of investing in our Soldiers, Civilians, and their Families.

Cyber Legion, Silent Victory, Change of Command

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

FORT EISENHOWER, Ga. – The Soldiers and Army Civilians of the 782nd Military Intelligence (MI) Battalion (Cyber Legion), accompanied by friends and Family, bid farewell to Lt. Col. Thomas Nelson and welcomed Lt. Col. Kirklin Kudrna, in a change of command ceremony hosted by Col. Benjamin Sangster, the commander of the 780th MI Brigade (Cyber), on Barton Field, June 1.

The Cyber Legion is comprised of more than 700 Soldiers and Army Civilians located across three states and three time zones who represent the Headquarters and Headquarters Company (Gladiators); A Company (Archers); B Company (Birds of Prey); C Company (Centurions); D Company (Dracones); and two operational detachments from Hawaii (Kopianas) and Texas (Cyber Rangers).

The change of command ceremony is a reflection of the procedures practiced since the birth of the United States Army in 1775 and encompasses the time-honored tradition of the passing of the colors by the battalion's senior enlisted leader, Command Sgt. Maj. Samuel Crislip, who is also referred to as the "keeper of the colors." The event signifies one officer's relinquishment of command and the incoming officer's assumption of the duties and responsibilities that come with command.

"As I sat down to collect my thoughts on what I wanted to say today, I honed in on making sure everyone here understood what a great accomplishment it is to lead the 782d because the Cyber Legion is not your ordinary battalion," said Col. Sangster. "It is one of only five operational cyber battalions in the United States Army, and more unique than that – unlike its sister battalions who are conveniently located on the same military installation – the Cyber legion is spread across three geographical locations and time zones: Georgia, Texas, and Hawaii; and to make matters even more complicated and unique, the Cyber Legion is responsible for presenting Combat Mission Teams and Combat Support Teams for four joint force headquarters – that's four general, flag officers, that all have the 782d on speed dial, as do the ARCYBER (U.S. Army Cyber Command), INSCOM (U.S. Army Intelligence and Security Command), and CCoE (Cyber Center of Excellence) commanders."

"Bottom line, the commander of the 782d has a lot of bosses, a lot of responsibilities, over 700 Soldiers and Civilians come to work every day, sometimes on nights and weekends, defending our country again nation-state adversaries," added Sangster.

Col. Sangster has known Lt. Col. Nelson since 2016 when he was the commander of the Cyber Training Battalion here and Nelson was serving as the 782d MI Battalion operations officer (S3) and later as a team lead for a Combat Mission Team. After his command in 2018, Sangster went on to serve as the Information Dominance Branch chief at Human Resources Command where he was responsible for overseeing the careers of all Cyber Soldiers.

"I was just getting to know the who's who of the Cyber Branch when it became very clear to me that Tom Nelson was one of our rising stars," said Sangster. "That was confirmed when Tom was selected to serve as the commander of the 782d and it was further confirmed when he was selected for senior service college.

"When I was selected for command of the 780th, it brought me peace of mind knowing Tom Nelson was one of my battalion commanders. In my observations over the years – he has a great reputation and I knew I had nothing to worry about with (him) leading the Cyber Legion."

"Tom, watching you up close for the last few years has just reaffirmed what I saw many years ago – you are an amazing leader who cares about his people. Thank you so much for leading the Cyber Legion the last few years. You've done an amazing job and we wish you the best of luck as you continue to serve our Army," said Sangster

Lt. Col. Nelson, in his remarks, discussed what he was most proud of coming out of command.

"The focus on people, mission, and balance, deliberately in that order," said Nelson. "The leader professional development over the last two years, the training of operators in FORGE, and the maturing of the cyber force shown by 308 basic, 116 senior, and 29 new masters qualifications in their work roles over the last two years."

Nelson also took time to acknowledge those responsible for his opportunity to command and to those who have made his command a success.

"Thank God, my family and the dedicated Civilians and Soldiers of the 782d MI Battalion," said Nelson. "Thanks to Maj. Gen. (Michele) Bredenkamp (Commanding General, U.S. Army Intelligence and Security Command), Col. (Matthew) Lennox, and Col. Sangster for this tremendous opportunity to lead they Cyber Legion these past 2 years."

Lt. Col. Nelson's next assignment is with the Cyber Center of Excellence (CCOE), the Cyber Proponent, where he will be the Deputy for the Office of Chief of Cyber and attend the Army War College distance learning.

Lt. Col. Kudrna is a Nebraska native and received his commission from Kansas State University ROTC in 2002. His most recent position was the Offensive Cyberspace Operations Mission Lead at the ARCYBER Technical Warfare Center. Prior to this position, he served as the Joint Force Headquarters – Cyber (Army) Military Deception Officer, integrating military deception (MILDEC) and military information support operations (MISO) into Army cyberspace operations.

Everywhere and Always…In the Fight! Cyber Legion, Silent Victory!

Innovation – Our Current Commissioned Officers and their Future

By CPT Diana Contreras, Operations Section Lead, DET HI, 782D MI BN (CYBER)

THE 782D MILITARY INTELLIGENCE BATTALION'S DETACHMENT in Hawaii has nine Commissioned Officers, each providing significant contributions, experience, and expertise that will shape the future of our force. These Officers have impressive operational and academic backgrounds. However, their greatest strength lies in the power of their leadership. While we know that innovation usually involves tools and technology, let us not forget: the bedrock of our force involves its people.

Recently, our Chief of Plans and Operations Section Lead learned valuable lessons in innovation when they became certified Military Scrum Masters. Innovation requires approaching a situation with a growth mindset, welcoming new ideas, and reaching an optimized solution. When we combine the various backgrounds and perspectives of our top-performing leaders, we will find our individuals innovating in ways we have not before.

Our Chief of Plans is a Captain with an undergraduate and master's degree in Computer Science. With an Infantry background and a passion for Cyber, he is undoubtedly well-versed in the technical systems we so heavily depend upon. Our Operations Section Lead is a Captain with an undergraduate degree in Mechanical Engineering. Her previous experience in Defensive Cyber Operations provides a challenging approach to her current offensive assignment.

When these two Commissioned Officers attended the Military Scrum Master course, they emerged with tools that drive our teams toward innovative thinking. Scrum, occasionally referred to as Agile Framework, is the pressure of getting a job done in a period of time, using the cumulative power of an entire team. This framework is usually applied in the context of software-development, but its applicability is extended when adopted to build successful teams. A key value instilled in this framework is "kaizen", which encompasses a spirit of a united team working together in small increments of improvement and change. When we push a team to new levels, we should not be valuing the processes and tools. Instead, the focus is the individuals and their interactions, collaboration, and responding to change effectively.

Some of the quirky habits instilled in Military Scrum Masters is to avoid saying the word "no" by replacing it with the words "yes, and". While a seemingly silly practice, this encourages teams to accept every idea and collaboratively mold it into a usable concept. Similarly, when providing constructive feedback, the framework recommends using the phrases, "I like…,I wish…and I wonder…". These phrases keep the focus on what is traditionally considered "sustains and improves" while maintaining a growth mindset. While these are short semantics that frame our communication, there are various in-depth methods techniques, roles, and concepts that the Scrum Framework transforms the way we manage our teams.

The concepts of Scrum and Agile Framework contain techniques to instill innovation, and these Commissioned Officers along with several leaders from other units have applied the Scrum framework in cyber operations. Although experience and expertise are of value, our leaders must understand that the careful application of our talents and personnel will determine success. For those interested in learning more, please reference the book titled "Scrum: The Art of Doing Twice the Work in Half the Time" by Jeff Sutherland. Our best teams require the leadership of innovative officers in order to collectively break barriers in order to succeed. ■

"Lessons Learned Shaping a New Mission Set"

By LTC Benjamin Klimkowski, MAJ Ken Woods, MAJ Richard Byrne, 11th Cyber Battalion

INFORMATION DOMINANCE PROFESSIONALS are living in an interesting time. Our branch has matured and is old enough that many officers have served exclusively in one brigade of the Cyber Mission Force. Arguably, these units have passed the inflection point where best practices, operating procedures, established training programs are readily available and there is an understanding at higher echelons on how to employ these units. While established units exist, the Army is investing heavily into new Cyberspace and Electromagnetic Activities (CEMA) and information operations organizations. In addition to the 11th Cyber Battalion's Expeditionary CEMA Teams (ECTs), the Army has set forth major initiatives such as Multidomain Effects Battalions (MDEBs) and Theater Information Advantage Elements (TIAEs) to integrate, synchronize, and execute CEMA into multidomain operations. Likewise, related Information Advantage Activities (IAA) such as SMDC's Theater Strike Effects Groups or USASOC's "Jedburgh team" concepts are calling on our Cyberspace and Electromagnetic Warfare (EW) officers to figure out how to incorporate CEMA into tactical concepts of operations. Into the foreseeable future, the probability that a young "17-series" officer will serve in a "new" CEMA organization is high—17s are going to be expected to innovate.

Understanding how to shape and innovate in these new settings is paramount. This article will highlight the role that leaders at the team level have in shaping a new mission set and will present advice to navigate the inherent challenges new mission sets present. The problem will be analyzed from the perspective of the team lead working with higher headquarters and from the perspective of building a team of diverse professionals to tackle the new mission set.

Challenges with higher headquarters.

"The operational level[1] of war in cyber is broken," quipped one senior officer. The year is 2018, and we had just received briefing after briefing at a classified symposium that highlighted the challenges over the previous year that teams and task forces had in planning, coordinating, and sustaining operations with their higher headquarters. The refrain is common; team leads universally felt that their operational controlling (OPCON) headquarters were not providing proper missions, orders, guidance, etc. Poorly scoped orders, whether incomplete or infeasible, were commonplace. Much of what these HQs were directing us to do was a poor use of highly skilled assets and not consistent with the vision of the team's concept of employment. As a new field grade trying to keep a group of young professionals motivated through these challenges, many of which are bureaucratic, shaping or "leading up" with your operational-level headquarters can be a frustrating experience.

Why is shaping operations at echelon so challenging? Planners at echelon cannot cleanly plan for what they do not understand. The Army establishes these organizations with concepts that are aspirational and are intended to adapt to future needs. Effectively, the concepts for these units are often vague and over-scoped without clear, concrete examples for the outsider to determine how to effectively plan. Moreover, the Army, partly because these efforts are embryotic, does not widely publish these new concepts in doctrine or leader education. This lack of documentation makes it difficult for the greater community to reference how to employ the asset. For new initiatives, the implications are that the team lead (or immediate field grade overseeing the unit) will be responsible for advising how to best employ a nascent asset to support larger efforts.

Obviously, team leads need to educate their higher and supported units and distinguish what makes the team unique. Beyond providing a unit overview, one of the most important things a leader can do for planners is to delineate a team or unit's capabilities from its functions. Here, capabilities refer to what the team can do in a broad sense as opposed to a specific hardware platform, software, or material means. For example, ECTs provide an expeditionary CEMA capability to a theater command— a lightweight, deployable means to perform electromagnetic warfare and cyberspace operations. Function, in this context, refers to what the vision intends the team to do with its capability. For ECTs, an example function would be multidomain reconnaissance to develop targetable information for future operations. The significance of outlining capabilities from functions helps planners avoid cognitive bias of employing the team based off what they have seen in the past or only looking at the team's capability to satisfy an immediate need. Our organizations are capable of much because we have such highly skilled individuals, but too many operations outside of the intended use pulls focus. Could an ECT use its expeditionary CEMA capability to perform digital force protection? Yes, but that use is not within the intended vision and is more likely appropriate for another theater IAA. Drawing the distinction of functions from capabilities will aid the team lead in navigating the inherent negotiations of building campaign plans with supported units. A final thought on this point: breaking through these preconceived biases and agendas can be difficult for an O-4 when the room is filled with O-5's and higher—it is wise to start delineating these sticking points early and often.

To help solve the problem of shaping missions with supported or higher commands team leads would benefit from employing an operational design[2] methodology. While "Op design" is typically associated with planning at echelons corps and above, it is a useful

planning framework to think through and understand loosely or ill-structured problems. Fundamentally, the goal of design is to develop an operational approach[3] through an understanding of the current operating environment (OE), its actors and their relationships; an understanding of what the command wants the OE to look like in the future; and the development of different ways to achieve that future state. Understanding the supported command is the first step in finding the nexus of what the supported unit needs and the opportunities that exist to help mature your organization.

Established planning paradigms and understanding are straightforward ideas, but they are nontrivial and unfold in subtle ways. First, a critical part of understanding is to appreciate organizational history, context, and the limits of your immediate staff counterparts. Each command has its flavor, idiosyncrasies, and blind spots that do not conform to doctrine. As a combatant command (CCMD) OPCON Cyber Protection Team lead, my adjacent team lead and I had trouble getting our command to take the next step in maturity and organize missions on the command's critical network infrastructure. After some time with our staff counterparts, it became clear that they lacked knowledge of what networks were most important to the organization's key missions. This issue was compounded by the fact that the traditional processes to garner the information from the service components would not have worked due to the unique nature of the number of joint task forces and contractors at play. The tipping point for us was to help the staff identify and decompose the network key terrain by analyzing each of the command's prioritized missions with the right stakeholders present. Second, op design helps ward off a "transactional" relationship with supported units, where the team is given one-off missions with little to no understanding of how the team will support the command long-term. If team leads are not careful, the staff will anchor on how to employ the team's capability to satisfy the command's immediate priorities, with not insight to how to build to a better mutually reinforcing relationship.

One way to motivate the team while dealing with external stakeholders is to "extend the team," i.e. bring your staff counterparts into your team's circle of trust. Often the non-lethal professionals within maneuver organizations get sidelined or are not able to assert themselves due to rank, experience, expertise. Find who the trusted agents are within a command (G3, G2, G6) and who needs work (often IO, CEMA, SOF LNO, etc). These individuals are key personnel to influence; make them feel like their input is valuable to both their own commander and your team. When successful, you will get buy-in, build trust and momentum across both sides, and make your team's job easier.

Finally, be a good steward and be patient. Educating the force is one of the more difficult things that you will do as part of a new effort. Often, teams are limited by time and resources (TDY budget, LRTC); constrained by the context of the training environment (venues were not intended for CEMA). Likewise, shaping updates to an operational plan (OPLAN) is challenging. In addition to the cumbersome enterprise of educating the planners to produce better plans, OPLAN updates themselves occur over the span of several years and personnel movement cycles. This fact necessitates an iterative process of "force education" to ensure the appropriate staff writes ECTs into the OPLAN. Change at echelon is not a quick process.

Building the team

Building a strong team is like building any other strong small unit. Team leaders need to have a solid vision for their people, they need to identify their key stakeholders, and they need to foster a team identity. Team leadership needs to get their personnel trained and achieve wins through exercises and operations. Like many of the leader challenges in this article, it is easily stated but difficult to execute.

New mission sets present two significant leadership challenges that are more pronounced than established units. First, new organizations have a way of magnifying and exacerbating common and routine problems. Things like meaningful counseling and communicating shared understanding are more strained due to the inherent uncertainty and volatile training schedules of new efforts. Leader engagement is vital; a disengaged leader is the kiss of death for a team working something new and innovative. Questions leaders that are executing new mission sets will need to answer are what are the acceptable levels of ambiguity and uncertainty? What does everyone fundamentally need to know? Being uncertain is okay, if everyone on the team is tracking exactly what is unclear and what leadership is doing about it.

Second, as we mature new organizations at the unit level and try to capture those experiences to improve the greater Army, the burden of innovation can weigh heavy. MG McGee, the former Deputy Commander of Army Cyber once stated, "it is really difficult to ask an organization that is operating at full capacity to simultaneously do those things and be innovative about new approaches."[4] This burden is readily apparent when trying to adapt existing Army training processes to a new collective and individual tasks. For example, following the eight-step training model, leaders need to take more time to prepare and assess new tasks than established military activities that can reference training circulars and organizational experience. Adept leaders will recognize and account for these challenges; if a leader naively demands the same level of perfection as organizations that have been around for decades, everyone is going to experience pain. Questions leaders executing new mission sets will need to answer are what is the acceptable level of immaturity and what is the unacceptability level of substandard performance? Rome was not built overnight. While nobody wants gaps in standard operating procedures (SOPs) and training programs, if a unit is consistently improving, then the leadership is steering it in the right direction.

Summary

Team leaders have an outsized role in ensuring the success of their team, the organizations above them, and improving the way the branch operates. In the absence

of perfect planning and resources, the leaders at the team level will pull together and make missions happen. Shaping at echelon and extending influence are key skills that can be cultivated with the right appreciation for how to integrate into the planning process and the right perspective. Building a team of highly skilled analysts and operators is also possible with a solid vision, engagement, and deliberate approach. As Andrew Marshall asserted, "rather than money, talented military personnel, time, and information have been the key resources for innovation," and that this talent exists within the in the military services.[5] Since its inception, the Cyber branch has consistently demonstrated this sentiment and will continue to do so.

References:

[1]Operational level of warfare - (DOD) The level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. (JP 3-0) Referenced in ADP 5-0, ATP 2-33.4.

[2]Operational design is the conception and construction of the framework that underpins a campaign or operation and its subsequent execution. The framework is built upon an iterative process that creates a shared understanding of the OE; identifies and frames problems within that OE; and develops approaches, through the application of operational art, to resolving those problems, consistent with strategic guidance and/or policy.

[3]Operational approach - (DOD) A broad description of the mission, operational concepts, tasks, and actions required to accomplish the mission. (JP 5-0) Referenced in ADP 1-01, ADP 3-0, ADP 3-07, ADP 5-0, ADP 6-0, FM 3-0, FM 3-24, FM 3-96, FM 6-0, ATP 3-13.1, ATP 3-21.10, ATP 3-21.20, ATP 5-0.1.

[4]Luc Dunn, "Talent Management: Acquire, Develop, Employ, Retain,"AUSA News, 30 AUG 2018. Accessed from *https://www.ausa.org/articles/talent-management-acquire-develop-employ-retain*

[5]Krepinevich, Andrew F., and Barry D Watts, *The Last Warrior: Andrew Marshall and the Shaping ofModern American Defense Strategy, 2015.*

Integrating DevOps into CSD-T

By CPT Andres Alejos, CPT Samuel Miller, CPT Tyler Reece, 11th Cyber Battalion

DEVELOPMENT OPERATIONS (DEVOPS) is the combination of philosophies, practices, and tools that increases an organization's ability to deliver applications and services to their customers at a more rapid pace.[1] At Cyber Solutions Development Detachment Tactical (CSD-Tactical), the detachment within the 11th Cyber Battalion specializing in Cyber Capability Development, we actively leverage the DevOps framework in multiple aspects. Firstly, it forms the core of our mission, enabling us to provide capability development in support of Army Cyber mission requirements. As we scale our workforce, DevOps also allows us to train our personnel to mirror real-world scenarios. Finally, we employ DevOps in an iterative fashion to tackle administrative requirements such as our new interview process, standard operating procedure (SOP) management, and metric tracking.

The time horizon of almost all CSD projects is less than six months. The nature of many of the projects leads to working hand in hand with the operational components of the Cyber force to gain a better understanding of their desired feature set and use cases. Considering the Cyber landscape is dynamic and fast-paced in terms of available opportunities, it is important for developers to employ a similarly nimble and dynamic development cycle. The predominant way this is done is through the implementation of the Agile methodology, using Scrum practices. Agile adheres to twelve core principles which emphasize the continuous reevaluation of goals with respect to current progress, such that if progress is either ahead of or behind schedule then the desired end state might have to change to account for those discrepancies.[2]

Team size plays a large role in the ability to adhere to the Agile principles, and as such, most projects consist of roughly five developers. Individual developers are responsible for implementing the features or improvements that they are assigned. This includes the responsibilities of designing, implementing, integrating, and documenting their contribution. Although senior developers bear more of the responsibility in planning and coordinating these contributions across the team, each developer is still required to understand how their piece fits in with the project. Development occurs in time units known as sprints which contain certain milestones such as planning, reviews, retrospectives, as well as daily standup meetings. Each of these milestones allow the stakeholder (in our case, usually Cyber operators) and developers to stay synchronized and have clear expectations of one another and share in a common vision of how to get to the desired end state.

The desire to plan training that more closely mimics project work has led to ongoing changes of how we conduct individual level JQR training. When CSD-T had only a handful of trainees at any given time, individual, tailored mentorship was possible. However, as we grow our organization to reach our eventual table of organization and equipment[3] (TOE) billeting of 120 qualified developers by FY26, our training approach had to adapt to meet the demands of scale. Instituting a training section to specifically manage both code review and administrative requirements of trainees as they progress through the Basic Developer job qualification record (JQR) was the first organizational step. Additionally, we added new control measures, moved all training project submissions and code review to GitLab to collect metrics more seamlessly. Finally, we created a series of gates, combined with recurrent counseling sessions, to ensure trainees are progressing steadily through the process.

The integration of DevOps practices even extends to certain administrative aspects within CSD-T, such as having an agile approach to SOP's and tactics, techniques, and procedures (TTPs) as well as implementing an interview process to identify developer talent within our battalion. The CSD-T SOP is a living document where individual members can make requests or raise concerns regarding the existing SOP, and site leadership – to include site OIC, NCOIC, Technical Director, and section leads – can review the request or comment. The SOP includes many TTPs and best practices, but those can also reside elsewhere as code, such as formatter files or continuous integration, continuous delivery (CI/CD) pipelines that enforce practices that are reflected within the SOP.

At the intersection of the DevOps ethos and Agile methodology and the day-to-day operations of CSD-T is the use of technologies to track and enforce the DevOps control measures. CSD-T's main weapon in this regard is the use of GitLab and all its components to tie the ideas expressed throughout this article to actual products and code. GitLab provides a suite of tools focused both on code production as well as team coordination and enables CSD-T to train and operate how we intend to fight.

During projects, we use GitLab repositories to store and manage versions of code. Within projects, we use GitLab Boards to manage requirements and load balance work across the team. We use GitLab's Code Review tool to provide feedback to developers and improve the quality of the code base. GitLab CI/CD is used to enforce the coding standards and testing requirements of CSD-T, as well as perform the requisite checks to ensure a product is ready for release once all features are integrated. GitLab Metrics enables CSD-T leadership to capture where their developers' time is being spent, and where adjustment is needed to meet mission requirements.

The training section uses GitLab Metrics to analyze student and trainer/mentor contributions, as well as using

GitLab as a delivery mechanism for training content. We can use GitLab Groups to organize our Cyberspace Capabilities Developers (CCDs) into different roles according to their sections as well as their JQR certification level. This enables certain access control measures, such as giving a Basic Certified CCD the ability to perform code review on a trainee as well as contribute new training material, while still requiring either a Senior Certified CCD or member of the leadership team to verify such contributions or officially sign off on a JQR line item. We use Gitlab Boards to manage code review for trainees. This enables us to have a clear picture of all trainee code submissions which require review, as well as tracking insightful statistics such as average time for code to be reviewed, and the top certified CCDs who are performing code review. We can then use this data to improve the methods we are using and measure their successfulness.

We also make use of GitLab to iterate over administrative documents. For our SOP, we allow anyone to create an Issue with suggested improvements, corrections, or questions. We conducted an initial CSD-T Vision Summit to make the first drafts of these administrative documents, with the expectation that from there on we could use features of GitLab to iterate on these documents in real-time without having to reconvene in the same way. We can use GitLab's formal Release utility to mark new revisions of the SOP to distribute to CSD-T. We keep artifacts such as CSD-T's structure and phone roster in various file formats, such as JavaScript Object Notation (JSON) and Comma Separated Values (CSV), which are easily ingested by scripts so that the SOP can stay current with personnel changeover as well.

The integration of DevOps practices and Agile methodologies has greatly enhanced the efficiency and effectiveness of operations within CSD-T. By adopting a dynamic development cycle and leveraging technologies such as GitLab, CSD-T has been able to stay ahead of administrative requirements and deliver applications to their customers at an accelerated pace.

References:

[1]Kim, Gene, et al. The Devops Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations. IT Revolution Press, LLC, 2021..

[2]Beck, Kent, et al. "The Twelve Principles of Agile Software." Principles behind the Agile Manifesto, Agile Manifesto Authors, *https://agilemanifesto.org/principles.html*.

[3]The table of organization and equipment (TOE) is an authorization document for personnel and equipment, establishing requirements given a specific doctrinal mission.

The Infrastructure Support Element (ISE) Uses Persistent Cyber Training Environment (PCTE) to Enable Growth

By CPT John Prukop, 11th Cyber Battalion

UNDERSTANDING DATA ENGINEERING, END-TO-END TRANSPORT OF INFORMATION, and appropriately securing a network are all specialties that the 11th Cyber Battalion (CYB) ISE aims to provide. Using PCTE provides a collaborative medium to integrate Electronic Warfare (EW), enable close-proximity Offensive Cyber Operations (OCO), and communicate with applicable Cyber Mission Teams (CMTs). The ISE has taken advantage of PCTE and its capabilities to include Hardware in the loop (HWIL) to provide realistic, scalable, and dynamic cyber training environments for cyber, signal, and intelligence professionals.

PCTE plays a significant role in enhancing TTPs throughout the Battalion and allows Soldiers, crews, and teams to work on skill development, team collaboration, assessments, and continuous learning. Crew Evaluations and Brigade Operational Readiness Assessments (ORAs) are vital opportunities to enhance these TTPs and accomplish mission-essential tasks. These tasks include establishing infrastructure operations and conducting Cyberspace Electromagnetic Activities (CEMA).

Four aspects of PCTE that enhance TTPs are skill development, team collaboration, evaluation and assessments, and continuous learning.

1. Skill Development: PCTE provides cyber, signal, and intelligence professionals with the opportunity to develop and refine their skills by emulating real-world networks they may encounter within the cyber domain (including grey and red space). These training scenarios reinforce the use of cyber professional tools and resources to stay abreast of the latest cybersecurity risks, attacks, and vulnerabilities. The ISE aims to provide additional opportunities through structured content plans, training courses, and assessments. These opportunities will enable current and future Soldiers within the ISE, Expeditionary CEMA Teams (ECTs), and other organizations to bolster knowledge based on new content. Some of the content currently in development includes a fundamental operator and an infrastructure development course. Once these courses are available, they can be shared with units that have similar training needs such as the Multi-Domain Task Forces (MDTFs). This effort will ensure that 11th CYB remains well-prepared to address emerging threats and remain current with the evolving cyber domain.
2. Team Collaboration: PCTE enables teams to train together in a simulated cloud environment, fostering collaboration and communication among team members. This collaborative training helps improve the team's overall TTPs and allows for various software or hardware to be tested. The 780th MI BDE's Operational Readiness Assessments (ORA) 23-03 demonstrated the ability of geographically dispersed ECTs and CMTs operating together.
3. Evaluation and Assessment: PCTE allows ECTs to assess their skills and abilities, identify knowledge gaps, and focus on techniques that need improvement. The 11th CYB has participated in two ORAs with the Cyber Mission Teams (CMTs) and outside organizations including the 7th Special Forces Group (Airborne) and Army Futures Command showcasing collaborative and assessment competencies. The ORA AARs provide feedback that has been invaluable in ensuring that the ECTs meet current cyber operational requirements per the current skill sets of the team's ability.
4. Continuous Learning: Cyber threats are constantly evolving, and network capabilities are evolving. PCTE provides a platform for continuous learning and updates, allowing the professionals within the 11th CYB to stay current with the latest developments in the field. This continuous learning involves multiple efforts to emulate target networks. PCTE supports "hardware in the loop" (HWIL) to merge physical and cloud environments. This feature greatly expands what is possible for training. The ISE's physical infrastructure allows for EW capabilities and OCO techniques that require proximity to be integrated within an established scenario. This scalable infrastructure allows the ECTs to refine their TTPs and showcase various system capabilities.

PCTE allows for persistent network access within a common training environment, which solidifies cross-organization collaboration. Since PCTE can be accessed from various locations this platform is a perfect medium for ECTs integration into ORAs. The use of PCTE is an essential component to updating ECT TTPs. PCTE enables effective cyber operations training. As the 11th CYB continues to leverage PCTE, Soldiers will be more proficient to handle their various work roles.

Soldiers Innovating Technology, Refining Tactical Concepts, and Strengthening Partnerships

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

SCHOFIELD BARRACKS, Hawaii. – Soldiers from the 11th Cyber Battalion, 780th Military Intelligence (MI) Brigade (Cyber), U.S. Army Cyber Command (ARCYBER) refined tactical Cyber-Electromagnetic Activities (CEMA) concepts for the Army during an Operational Readiness Assessment here in late March 2023.

For the event the 11th Expeditionary CEMA Teams (ECTs) employed innovative technology with assistance from experts from the Army Cyber Institute (ACI) at the U.S. Military Academy at West Point, the Army Program Executive Office – Intelligence, Electronic Warfare and Sensors (PEO IEW&S) and industry partners, along with training with the Combat Mission Team, Detachment-Hawaii, 782nd MI Battalion (Cyber).

The command teams from the 11th and 780th also used the time here to strengthen partnerships and discuss future collaboration with U.S. Army Pacific (USARPAC) and 25th Infantry CEMA experts and USARPAC's Multidomain Effects Battalions (MDEBs).

"It's an amazing story for ACI, because it shows how quickly they were responsive to an operational force asking for support," said Col. Ben Sangster, commander of the 780th Military Intelligence Brigade (Cyber). "The bigger story is that you have the ECT out here practicing and innovating their tradecraft and abilities in the backyard of USARPAC."

The 11th is the Army's premier expeditionary CEMA battalion. Officially activated on October 16, 2022, the battalion can deliver a range of non-lethal, non-kinetic effects – including offensive cyberspace operation (OCO) and electronic warfare (EW) capabilities. Currently the 11th CYB has three companies and four ECTs. A fifth ECT is being planned by the end of Fiscal Year 2023, and by FY 2027, the 11th CY BN is projected to have a total 12 ECTs capable of providing OCO, EW, and information advantage functions and capabilities.

For this tactical demonstration, Soldiers from ECT-01 partnered with their ACI, PEO IEW&S, and industry partners. Although there was a culminating exercise for Maj. Gen. Neil S. Hersey, ARCYBER Deputy Commanding General – Operations, there were numerous other engagements throughout the week with USARPAC's CEMA and MDEBs, the 25th ID CEMA, and other military intelligence and signals intelligence units.

"In addition to integrating with the 780th MI Brigade's Combat Mission Teams, the biggest objective is to innovate with the greater community of interest. We have made considerable headway with ACI, working with the vendors, PEO and the generating force, and the EW community. Plenty of room for growth, but we're seeing this collaboration accelerate." said Lt. Col. Ben Klimkowski, the 11th's commander. "We are also trying to understand their needs (USARPAC and 25th ID CEMA and MDEB), to identify and shape what opportunities exist between the commands."

While partnerships are critical, the success of the engagements lies primarily on the innovation of the Soldiers, he added.

"We are breaking paradigms here where we are not getting a fielded, complete system with a tight training circular, and a tight understanding of what this system does," said Klimkowski. "We have smart analysts, operators, and developers working together to extend the capabilities and use them in ways that are very powerful. Our Soldiers make it look easy, but it is not normal; the 11th Cyber Battalion has a unique mission and culture where incredible talent like what you see here can flourish. It's really the technicians with the expertise and initiative that are refining and extending capabilities– not just employing– and using existing technologies in ways that were not initially envisioned."

The 11th CY BN currently supports mission planning and operational requirements across three continents and the Pacific Rim in direct support of 1st Special Forces Command, United States Army Pacific Command, and United States Army Africa and European Commands.

"What we are seeing is the future of Expeditionary Cyber Operations. These Soldiers are demonstrating proximal access via EW, air-launched, and ground-launched drones, which will be critical to achieving cyber effects during large scale combat operations in support of Army 2030 and beyond," said Command Sgt. Maj. Jesse Potter, the 780th's senior enlisted leader. "Some of these Soldiers never believed they would arrive via helicopter and then move tactically enabling cyber operations; let alone executing their operations with a drone or SPOT the Robotic Dog."

"The 780th is working with the operating force, the generating force, and institutional research agencies, like ACI, to provide value back to the Army," added Klimkowski.

SCHOFIELD BARRACKS, Hawaii – 2nd Lt. Joe Larouche, mission commander for the 11th Cyber Battalion's Expeditionary Cyber-Electromagnetic Activities Team-01, communicates with his higher headquarters about his team's mission, while Staff Sgt. Ryan Hedgcoth, Expeditionary CEMA operator, keeps an eye on security, during an Operational Readiness Assessment for the battalion here, March 30, 2023.

SCHOFIELD BARRACKS, Hawaii – Sgt. James Hyman, Expeditionary CEMA operator for the 11th Cyber Battalion's Expeditionary Cyber-Electromagnetic Activities Team-01, collects information from two sensors – on an unmanned aerial system and a robotic dog named Spot – to conduct cyber effects operations, during an Operational Readiness Assessment for the battalion here, March 30, 2023.

SCHOFIELD BARRACKS, Hawaii – Chief Warrant Officer 4 Aaron Foster, senior technical advisor, Cyber Solutions Detachment-Tactical, works on an Electronic Warfare Planning and Management Tool, during an Operational Readiness Assessment for the 11th Cyber Battalion here, March 30, 2023.

17D: Review and Way Forward

By LTC Chuck Suslowicz, Director, Cyber Solutions Development, 780th MI BDE (Cyber)

THE CYBER BRANCH plans, integrates, synchronizes, and executes cyberspace and electromagnetic warfare operations. The officers of the Cyber Branch are grouped into three different areas of concentration (AOCs) to more effectively accomplish these core tasks: 17A (Cyber Warfare Officer), 17B (Cyber Electromagnetic Warfare Officer), and 17D (Cyber Capabilities Development Officer). Cyber officers can, and do, move between these AOCs during their career depending on availability and appropriate training. 17D is the 'youngest' of the three AOCs and this article will provide an overview of the AOC, a brief retrospective on its early successes, and an outline for its trajectory moving forward.

The 17D AOC was initially created by a Notification of Future Change (NOFC) approved in October 2020 for implementation in October 2021. In October 2021, the first officer positions were converted to form the initial 17D positions across the 780th Military Intelligence Brigade (Cyber), the Cyber Protection Brigade (CPB), U.S. Army Cyber Command Headquarters, and other units. These officers were aligned against existing formations where their experience and knowledge in the development of cyberspace capabilities could provide immediate value and support to ongoing offensive and defensive cyberspace operations.

For example, nearly all officer positions related to 780th's Cyber Solutions Development (CSD) were converted to 17D, formalizing the previously implied focus of those positions on capability development rather than broader cyberspace operations. This focus resolved a problem recognized at the time of the original NOFC that effective capability development would require a cohort of officers to focus on the knowledge, skills, and abilities tied to capability development and a career track would be necessary to ensure those officers were able to build the expertise required to meet the capability development requirements of ongoing cyberspace operations.

Since October 2021, the 17D AOC has had multiple successes. The pilot 17D Basic Officer Leaders Course (BOLC) graduated in the fall of 2021. These officers were identified during the accessions process to have the potential to flourish as capability developers and the pilot was executed as the Army prepared to implement the AOC. The BOLC course material prepared them for the U.S. Cyber Command (USCYBERCOM) Cyberspace Capability Developer (CCD) Joint Qualification Record (JQR) standard and ensured that graduates would be able to immediately contribute as qualified developers upon arrival to their first assignment. Three classes later, 17D BOLC graduates are critical contributors to capabilities across the ARCYBER footprint while the schoolhouse has worked closely with the operational force to ensure prospective 17D's meet the same standards or are redirected toward an alternative AOC.

Once arrived at a unit, 17Ds fill several roles in the capability development process. Junior officers focus on technical mastery serving as members of development crews and core contributors to specific projects. This is a critical period for officers to gain the technical "reps and sets" to prepare them for a Senior CCD qualification, work hand in hand with 170D Warrant Officers, and gain initial experience with agile development processes. As captains, 17Ds serve as crew leads and section leads across ARCYBERs development organizations. They interface directly with supported organizations, refine requirements, design solutions, and assist in the implementation of core components of capabilities. If not already a Senior CCD, captain 17Ds finish up their remaining requirements or begin the long road toward Master qualification.

Field grade 17Ds currently serve as development site leads and director positions. These officers leverage their experience to guide the development of dozens of projects, work closely with supported organizations to refine complex requirements, and interface with ARCYBER and program offices to better meet the operational cyber force's needs. The initial establishment of 17D billets did not fully flesh out all field grade positions for the AOC, so work is ongoing to best identify where 17D majors, lieutenant colonels, and a small number of colonels will best serve the force beyond currently identified billets. Most likely, these positions will be associated with the capability approval process, oversight of the CCD work role, 17D training, and coordination with other commands such as Army Futures Command.

The 17D AOC is still rapidly maturing. It is approaching its expected manning for junior grades but is still woefully short field grade officers. Significant work has been done with the Air Force to refine the USCYBERCOM CCD work role standards, and when published, the updated JQR will better reflect the technical core competencies of the AOC. Similarly, the operational 17D community is working closely with Office Chief of Cyber (OCC) on the 17D accessions process to ensure suitable cadets are selected for each year's BOLC cohort. This effort has created a specialized interview process leveraging operational 17D captains for technical interviews and improved outreach to prospective cadets through events like the U.S. Military Academy's Cyber Leader's Conference.

The Army has created a unique AOC to support cyberspace operations challenge of rapid capability development in support of ongoing operations. 17D's have demonstrated the ability to meet this challenge both technically and as leaders of technical formations focused on the delivery of critical capabilities. Moving forward, the AOC will continue to work closely with OCC on the 17D accessions

process, update and refine the positions expected for field grade 17Ds and continue to work closely with the other services on the joint CCD standards. The Army's need for cyberspace capabilities will continue as long as cyberspace operations are necessary. Every interested officer is welcome to contact any 17D and tackle the CCD JQR. Those that are successful should consider a tour in a 17D position to gain a different perspective on cyberspace capabilities and broaden their understanding of cyberspace operations.

Persistent Adaptability: Innovation in the Army National Guard Cyber

By LTC Daniel Byrnside, Commander, TFE VII, 125 CPB

PRE-DATING THE FORMATION OF THE UNITED STATES AND EVERY BRANCH OF SERVICE, the Army National Guard was the nation's first organized fighting force, originating on December 13th, 1636, in the Massachusetts Bay Colony. Since that time the organization has evolved in various permutations and structure until arriving at its current state as a force provider with National Guard units in every state, territory, and the District of Columbia; all administratively overseen by the National Guard Bureau (NGB). Using its unique capability to serve both as a Title 32 organization in service to state-side support missions (counter-drug, natural disaster response, etc.) and as a Federal Title 10 active-duty element in support of national mission requirements, the National Guard has long been an integral part of the overall defense strategy of the United States, including its most recent support to Cyber Operations.

The creation of U.S. Cyber Command (USCYBERCOM) in 2009 (and the corresponding service component commands a year later) was a significant advancement in the command and control of the nation's operational cyber forces. To further augment the growth of U.S. Army Cyber Command (ARCYBER), cyber force structure was included into growth plans for the National Bureau and the U.S. Army Reserves shortly after the organization stood up in 2010. This growth allowed for ARCYBER to have an operational reserve force readily available to support their mission requirements as needed, culminating in the creation of Task Force Echo and the Kodiak Cyber Operations Team (later renamed to Cyber Warfare Company). These teams have brought unique National Guard capabilities to the forefront, relying on a wealth of private industry information security experiences across all business sectors and ensuring cutting edge technology and practices are employed on ARCYBER operational assets to best ensure mission success.

The Army National Guard continues to drive these missions forward, using existing operational experiences from previous mobilizations and applying innovative technological enhancements to critical assets to reduce operational overhead and minimize unanticipated activity in the conduct of operations. With the recent access of Title 10 virtual training environments, modifications to professional military training (PME) at the Cyber Center of Excellence (CCoE), and maturation of the National Guard's force structure, National Guard Soldier have never been more postured to support active cyber operations. As we look to the future of cyber support from Component 2 organizations, we see agile teams ready to assume increased capabilities and missions across the spectrum of cyber operations.

Evolution of Cyber Operations in the National Guard

As advances in technology have accelerated in the past several decades, the National Guard has worked closely with national level DoD assets to help achieve strategic objectives in the cyber domain. These efforts have gone back as far as the Virginia Army National Guard's Data Processing Unit (DPU), which was formed in 1975 and has been supporting data processing and cyber network defense missions for the NGB, NSA, and ARCYBER ever since. With the creation of ARCYBER in 2010, the National Guard Bureau was directed to build out a corresponding cyber force structure, resulting in the activation of the 91st Cyber Brigade (VA Army National Guard) in 2017, along with five Cyber Protection Battalions (CPB) spread across Virginia (two CPBs), South Carolina, Massachusetts, and Indiana and 11 Cyber Protection Teams (CPTs) spread across the nation. Conception of the 91st Cyber Brigade started in November 2016, was approved in February 2017, and activated in September 2017, incorporating the DPU and making it one of the fastest implementations of force structure in National Guard history. Ultimately, that speed was necessary for the activation of Task Force Echo (TFE) I on August 22, 2017, with the 123rd CPB assuming responsibility for the mission set from the 169th CPT. Alongside the creation of TFE came the Kodiak Cyber Operations Team (KCOT) (which evolved into the Cyber Warfare Company) out of a request for forces from Joint Force Headquarters-Cyber (Army) to support the Cyber Mission Force (CMF) with Information Operations and Full Spectrum Cyber Operations. These missions have continued in annual rotations since then to the current iteration of TFE 7.

Operational cyber support from the National Guard has not been without its challenges; however, many of which stem from a fervent mobilization pace, access to Title 10 training, and maturation from a force structure that was rapidly activated. Demand signal for cyber forces is seen throughout all components of the military, requiring frequent mobilization periods of 400 days with a 40-month dwell period in between, hindering opportunities to attend schooling while attempting to achieve stabilization with families and private industry careers. Additionally, access to Title 10 courses has been limited beyond standard PME courses as many of those opportunities are locked for Soldiers assigned the CMF, primarily due to limitations in instructor availability and force growth for active duty formations. Access to the courses prior to mobilizations is critical to reduce operational downtime due to training. Finally, due to the rapid creation of the National Guard cyber force structure, stabilizing units quickly formed

from adjacent formations in the various supporting states has had a long-term detrimental effect on achieving DMOSQ, with many formations just now getting within NGB-directed readiness.

In addition to the challenges above, Soldiers serving in National Guard Cyber formations face many of the same career demands as their active-duty counterparts, be it maintaining technical proficiency in an ever-changing cyber domain, achieving (and maintaining) CMF Joint Qualification Standards (JQS) for their work roles, or working through the various accesses and clearance requirements our cyber and military intelligence careers require of us. These challenges are inherent in our efforts to constantly innovate in order to ensure information dominance over our adversaries, and the National Guard serves as a unique asset to bring new and enhanced capabilities to bear for ARCYBER. These strengths have long been found across National Guard formations, be it the Soldier who serves as an electrician in his private industry job building out the wiring for a rudimentary forward operating base in Iraq, or the cyber NCO who is the lead security engineer for a water treatment facility providing in-depth ICS/SCADA training or operational support to the CNMF. The National Guard's ability to provide innovation in the cyber domain stems from its organic development of citizen Soldiers and remains one of its greatest strengths.

Innovations in Training and Recruitment

When not executing a Title 10 mobilization, National Guard Soldiers in the 91st Cyber Brigade have a variety of tools at their disposal to maintain proficiency in cyber operations, primarily built around effective cyber training ranges and utilizing the natural training talent of the NCO and Warrant Officer Corps to provide Soldiers with the latest technical skills. As it pertains to cyber training ranges, the primary capability utilized in the early years of the 91st Cyber Brigade and its supporting CPBs was ShadowNet, a Title 32 funded infrastructure managed by the 91st Cyber Brigade S-6 shop and made available for all Soldiers within the Brigade's force structure. With the maturation of the Persistent Cyber Training Environment (PCTE) and its utilization on Title 10 infrastructures for Federal mission sets, the focus of cyber training environments has since shifted, with the majority of National Guard cyber Soldiers now utilizing PCTE for their training scenarios on drill weekends. These training scenarios are further enhanced with customized capabilities intended to support training built out by NCOs and Warrant Officers (on occasion Officers) who bring their civilian skill sets to bear on instruction periods for emerging technologies and existing toolsets used by the CMF.

National-level exercises are another way that the cyber forces in the National Guard maintain their proficiency, typically being utilized as culminating training events for collective training. The largest among these has historically been Cyber Shield, an annual cyber training event held at multiple locations throughout the United States from year to year that allow CPTs and CPBs the opportunity to conduct validation exercises (for the CPTs) or culminating training events to validate readiness to support state missions (for the CPBs). Previous iterations of Cyber Shield have included events focused on responding to attacks on critical infrastructure (to include working alongside the actual private sector partners) and defending simulated state IT infrastructure from malware infections. These events, along with several other regional cyber exercises such as Cyber Yankee, Cyber Fortress, and Jack Voltaic have afforded the National Guard cyber forces ample opportunity to take their individual and collective training to the next level and validate their readiness to support state and federal missions.

The National Guard has also been innovating in the fields of recruitment, using existing Army recruitment methodologies tied to unique technical training opportunities to further increase the appeal of joining the Cyber Corps. Formations across the 91st Cyber Brigade have established outreach and memorandums of understanding with numerous education and government institutions to improve recruitment. Notable among these is the 125th CPB (supporting the current TFE mission), which has established relationships with The Citadel's DoD Cyber Institute along with the University of South Carolina (USC) to identify ways of continuing to attract talent to the National Guard's cyber forces, along with building capabilities within the state workforce to increase cyber security and improve incident response capabilities in support of the citizens of South Carolina. Additionally, the USC Aiken campus is in the process of building out a $30 million Cybersecurity complex that will include a Readiness Center for the 125th CPB along with classrooms and a testing area in private/public partnership with the Savannah River Site to grow cyber security readiness across the state. All these efforts have had an overwhelmingly positive effect on recruitment, with cyber Soldiers regularly joining the ranks from recruitment centers across the state, along with Soldiers transitioning from active duty to the National Guard.

Future Outlook and Challenges

As we look to the future of innovation in the cyber domain with the National Guard, a major focus centers on maintaining our adaptability to respond to changes in the operational environment. These changes are not just changes in technology but reflect organizational changes within the CMF as well as the ever-changing landscape of training requirements to maintain JQS or technical proficiency in a specific skillset. In the near future, it is anticipated that the growing pains of creating new force structure will (or already have) begin to dissipate as more of the Soldiers within the National Guard cyber formations achieve cyber branch equivalency or come into the force as newly trained 17As and 17Cs from the Cyber School. As it stands right now, almost every single new lieutenant and junior enlisted Soldier slotted in a 17-series billet in the CPBs and CPTs has completed their initial training at the Cyber School, slowly reducing the amount of equivalency packets submitted. Maturation of the force has come somewhat slowly, but focused efforts by leaders to enforce DMOSQ school

attendance with risk of removal from the CPB has borne fruit as readiness has increased dramatically.

Recruitment for positions at the CPTs and CPBs has been at consistently positive levels despite the recent recruiting challenges across the Army. The broad appeal of the Cyber Corps in the National Guard has hinged primarily on shared firsthand experiences of Soldiers who have converted to cyber MOSs and built new lives and careers on the positive experiences, training, and certifications gained from joining their state's CPTs or CPBs. This word of mouth has grown far outside of those organizations and has attracts established professionals from across Signal and Military Intelligence communities to shift their focus to joining the ranks of the National Guard cyber forces. From these changes we have seen Soldiers arrive at the unit with non-technical professional careers, focus a passion for learning into technical excellence, and drive that change into their private industry careers to change their professional careers. From a Certified Public Accountant becoming one of CWC's talented Mission Commanders to a construction worker achieving their first security certification and working towards a career in cyber, the National Guard's history of adaptability ensures it ability to meet new challenges with a strong and capable workforce.

The future is not without its challenges; however, and many of those challenges center around ensuring that the National Guard maintains close visibility of pending mission changes and adapts accordingly to meet the requirements sent by ARCYBER and USCYBERCOM. Expected changes are already in motion, with Task Force Echo's mission shifting to Marine Corps Forces Cyberspace Command (MARFORCYBER) in the next year alongside increased demand for CWC support to JFHQ-C, currently "the most operationally active unit" in that formation (BG Paul Craft, 2023). Future mission support requests from ARCYBER are in development, and the 91st Cyber Brigade remains in close coordination with the ARCYBER Reserve Affairs Office to ensure their downtrace CPB's organizational structure reflects those changes with sufficient time to adjust their Table of Distribution and Allowances (TDA) in time to support the required timelines.

Conclusion

Securing, defending, and responding to attacks on our nation's defense networks is a critical task assigned to USCYBERCOM and the NSA/CSS. Ensuring we have competent and trained cyber warriors ready to defend forward and take the fight to our adversaries is of the utmost importance to the overall national defense strategy and one the National Guard is prepared to support. Throughout the short (but operationally very active) history of the 91st Cyber Brigade, cyber warriors from around the nation have answered the call, working tirelessly around their private industry careers and family obligations to dramatically increase the readiness of the National Guard as a force provider of cyber warriors. That effort will continue in the future as well, as we continuously seek improvement and develop new and innovative ways to resolve challenges in the cyber domain. We look forward to continuing to work with ARCYBER and USCYBERCOM in all our future endeavors. Victory in the Shadows, For Freedom!

Army National Guard Soldiers receive medal from Ambassador of the Grand Duchy of Luxembourg

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

WASHINGTON –Soldiers from the 125th Cyber Protection Battalion (CPB), S.C. Army National Guard, received the Marche de Diekirch medal from her Excellency Nicole Bintner-Bakshian, Ambassador of the Grand Duchy of Luxembourg to the United States, at the Embassy of the Grand Duchy of Luxembourg in Washington, April 5.

The 125th CPB is currently deployed to Fort George G. Meade, Md., and Fort Gordon, Ga., as part of Task Force Echo (TFE) under the operational control of the 780th Military Intelligence Brigade and conducts cyberspace operations in support of U.S. Cyber Command (USCYBERCOM) and the Cyber Mission Force (CMF).

Marche Internationale De Diekirch is an international march, originally organized by the Luxembourg Army in 1968. The annual event consists of a 20k, 40k and even the 80k hike, and the foreign medal is authorized for Soldiers to accept and wear on their dress uniforms.

According to Command Sgt. Maj. Timothy Larkin, the battalion's senior enlisted leader, the award ceremony – at the Luxembourg Embassy in Washington, with the foreign medals presented by the ambassador – has been a highlight of the Soldier's deployment.

"Events like this one offer an opportunity to reflect and remember that Luxembourg and the United States are steadfast allies and close partners through our joint commitment to peace, security and promoting shared values of respect for human rights and democracy. This relationship is deeply rooted in feelings of gratitude towards the US soldiers who liberated Luxembourg twice from foreign oppression in 1918 and in 1945, and in appreciation to all those who contributed to Luxembourg becoming the free and prosperous country it is today", said Ambassador Bintner-Bakshian.

The TFE VII formation, primarily assigned to the 125th CPB, is composed of ARNG Soldiers from South Carolina, California, Michigan, and Ohio, with additional Soldiers in the Task Force from Georgia, Indiana, Louisiana, Maryland, Nevada, and Virginia. TFE VII is commanded by Lt. Col. Daniel Byrnside, commander of the 125th CPB, with Larkin as the senior enlisted leader.

"The Marche de Diekirch was a great opportunity for us to build camaraderie as a team, and being presented with the medal by the ambassador was a very unique experience, as well as the hospitality shown to us by the Luxembourg Embassy," said Chief Warrant Officer 3 Justin Bailey. "This was a once in a career opportunity and I'm very grateful for everyone who made it happen!"

WASHINGTON – Soldiers from the 125th Cyber Protection Battalion (CPB), S.C. Army National Guard, received the Marche de Diekirch medal from her Excellency Nicole Bintner-Bakshian, Ambassador of the Grand Duchy of Luxembourg to the United States, at the Embassy of the Grand Duchy of Luxembourg in Washington, April 5.

780th Military Intelligence Brigade (Cyber) Best Squad Competition

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

FORT WALKER, VA. – The Soldiers from B Company, 782nd Military Intelligence (MI) Battalion (Cyber), will represent the 780th MI Brigade (Cyber) at the U.S. Army Intelligence and Security Command (INSCOM) Best Squad Competition (BSC), April 19 through 24.

The winning team consisted of Staff Sgt. Aaron Fox, Sgt. Micheal Duli, Spc. Tanner Casey, Spc. Keaton Posey, and Pfc. Nathen Weaks.

"The Best Squad Competition is the culmination of the Sergeant Major of the Army's initiative of 'This is My Squad,'" said Command Sgt. Maj. Jesse Potter, the Brigade's senior enlisted leader. "We still select our NCO (noncommissioned officer) and Soldier of the year from the competition but everything within the competition is team based. It drives home the role of the NCO in training, preparing and leading their Soldiers."

"The Squad representing 782d MI BN found out during day two that they still needed to compete even when they have one of their teammates go down," added Potter. "They finished the competition with only a four-Soldier Squad and was able to adapt, overcome and ultimately win the competition."

Staff Sgt. Fox, the squad leader, is a Target Digital Network Analyst (TDNA) and graduated from Nansemond River High School, Suffolk, Virginia. Fox earned the Airborne and Air Assault badges, is Combatives Level 1 certified, and a graduate of the Special Warfare SIGINT (signals intelligence) Course, Mode 1, Combat Lifesaver (CLS), Basic Leaders Course (BLC), and Advanced Leaders Course.

"I trained and mentored the Soldiers of my squad to enhance their knowledge and skills and improve my leadership capabilities," said Fox. "I wanted to be a Paratrooper/Soldier from a young age after watching my father's jumps. I plan to earn the Expert Soldier Badge, Pathfinder Badge, and Ranger Tab. I also plan to join 75th Ranger Regiment after my time as a Drill Sergeant at Fort Huachuca, Arizona. When I get back to an Airborne position, I want to become a Jumpmaster and earn the Master Parachutist Badge."

Sgt. Duli is a Target Analyst Reporter and Training NCO (noncommissioned officer) from Pittsburgh, Pennsylvania. Duli graduated from Plum Borough Senior High and attained a bachelor's in chemical engineering from the University of Pittsburgh. He is also a CLS and BLC graduate.

"I enjoy competing with the best the unit has to offer to see how I stack up," said Duli. "My future goal is to go through the Army's Green to Gold process, get my master's degree, and commission as an officer."

Spc. Casey is a Cyberspace Operations Specialist who hails from Harker Heights, Texas and graduated from Harker Heights High School. He also attained a Criminology and Criminal Justice degree from the University of Nebraska.

"I am competing to further my experience in the Army and to build better teamwork and bonds in my squad," said Casey. "I would like to recognize my wife. Without her support I would not be where I am today. My role models are my parents because they taught me what it means to be a good person and that helped me to become a good Soldier."

Spc. Posey is a TDNA from Salinas, California and graduated from Pacific Grove Adult School and has a CLS certification.

"I always appreciate a challenge where I am able to test my physical abilities and my knowledge," said Posey. "Even if the outcome is not what I desired, there is always something to be learned by participating."

Posey's future goals are to attend the U.S. Army Air Assault, Airborne, and Ranger schools, achieve the rank of sergeant, and obtain his bachelor's degree in data science.

Pfc. Weaks is a Digital Network Exploitation Analyst (DNEA) from Decatur, Illinois and graduated from Decatur Christian School.

"My future goals are promotion to specialist and then sergeant, and then eventually become a cyber warrant officer. I also want to become a tool developer," said Weaks. "I would like to recognize my wife for supporting and encouraging me. I would also like to recognize my brother Sgt. Jonathan Weaks; brother-in-law Staff Sgt. Michael Deremiah; dad, Tom Weaks; and father-in-law, Tom Michael, who are all either prior service or active duty for all of the advice and support that they have given me."

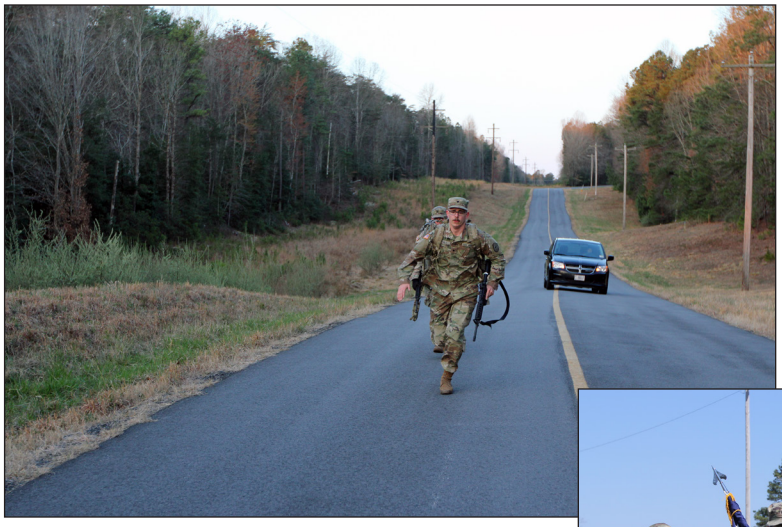
The Brigade's BSC events included: a modified Army Combat Fitness Test; day and night land navigation; the obstacle course; M4 rifle zero and qualification, M17 pistol qualification range; 12-mile ruck march w/ four Soldier tasks; and a command board.

In addition to Best Squad, the 782d MI Battalion Cyber Legion Soldiers swept this year's competition as Sgt. Duli is recognized as the Brigade Noncommissioned Officer of the Year, and Spc. Posey, the Brigade's Soldier of the Year.

Praetorians. Cyber Legion.
"Strength and Honor" "Everywhere and Always…In the Fight!"

FORT WALKER, Va. – The 780th Military Intelligence Brigade (Cyber) hosted their Best Squad Competition (BSC) here March 27 through 31 to determine who would represent the Brigade at the U.S. Army Intelligence and Security Command BSC. The first day's events included a Physical Fitness Assessment including the Hand Release Pushup, Sprint-Drag-Carry, and the two-mile run, as well as the day and night land navigation courses.

FORT WALKER, Va. – The 780th Military Intelligence Brigade (Cyber) hosted their Best Squad Competition (BSC) here March 27 through 31 to determine who would represent the Brigade at the U.S. Army Intelligence and Security Command BSC. The second day of the Brigade BSC included the M4 rifle zero and qualification, M17 pistol qualification, and disassemble, assemble and functions check of the M4 rifle, as well as A.P. Hill obstacle course.



FORT WALKER, Va. – The 780th Military Intelligence Brigade (Cyber) hosted their Best Squad Competition (BSC) here March 27 through 31 to determine who would represent the Brigade at the U.S. Army Intelligence and Security Command BSC. The third day of the BSC started with a 12-mile ruck march including four Soldier tasks.

FORT WALKER, Va. – The Soldiers from B Company, 782nd Military Intelligence (MI) Battalion (Cyber Legion), will represent the 780th MI Brigade (Cyber) at the U.S. Army Intelligence and Security Command (INSCOM) Best Squad Competition (BSC), April 19 through 24.

The winning team consisted of Staff Sgt. Aaron Fox, Sgt. Micheal Duli, Spc. Tanner Casey, Spc. Keaton Posey, and Pfc. Nathen Weaks.

780th Military Intelligence Brigade (Cyber) - Engagement Events

CHICAGO, Ill. – Soldiers from the 780th Military Intelligence Brigade (Cyber) supported a job fair at the Chicago Cyber Conference hosted by the Illinois Institute of Technology, March 31. 1LT Graham Webb, a cyberspace operations officer, and SGT Gegory Braveboy, a cyberspace operations noncommissioned officer (NCO), engaged undergraduate and graduate students from Illinois Tech, along with a few ROTC cadets. For the second year, they were the last table in the hall to have people still waiting and wanting to complete the challenges.

LAS VEGAS – Soldiers from the 780th Military Intelligence Brigade (Cyber) and the Cyber Protection Brigade supported U.S. Army Recruiting Command in engaging more than 2,000 high school students from the local area and told them about the life-changing opportunities of Army service, March 21 and 22.

LONG BEACH, Calif. – Soldiers from the 780th Military Intelligence (Cyber) supported U.S. Army Recruiting Command (USAREC) by talking to people about the Cyber and Military Intelligence Branches and telling them about the life-changing opportunities of Army service at the Acura Grand Prix of Long Beach, April 14 and 15.

According to MAJ Jacob Curtis, team lead, Detachment Hawaii, 782d Military Intelligence Battalion (Cyber), the Brigade's Soldiers assisted in generating more than 1,300 leads – more than double the number from the same event last year – with the majority coming from K-12 students on a field trip.

ROCKFORD, Ill. – Soldiers from the Cyber Protection Brigade (Hunters) and the 780th Military Intelligence Brigade (Cyber) are supporting U.S. Army Recruiters from the Loves Park Recruiting Company April 24 through 28 to increase awareness in Northern Illinois area schools about the diversity of career fields within the Army and to assist Recruiting NCOs in developing potential enlistments.

FORT GEORGE G. MEADE, Md. – Soldiers and Civilians representing 780th Military Intelligence Brigade (Cyber) and Task Force Echo participated in the Anne Arundel County Public Schools (AACPS) Meade Cluster Spring Event and engaged several hundred members of the local community, April 29. There were a lot of young people and parents interested in cyberspace (and Military Intelligence – it is a partnership) and we hope to see them again at the Hackathon event we sponsor with the Anne Arundel County Public Library Odenton Branch this fall.

GAMBRILS, Md. – (Arundel High School STEM) Soldiers from the 780th Military Intelligence Brigade (Cyber) engaged students from Arundel High School to encourage their interest in STEM (science, technology, engineering, and math) and to tell them about the life-changing opportunities of Army service, May 17. #beallyoucanbe #ArmyPossibilities

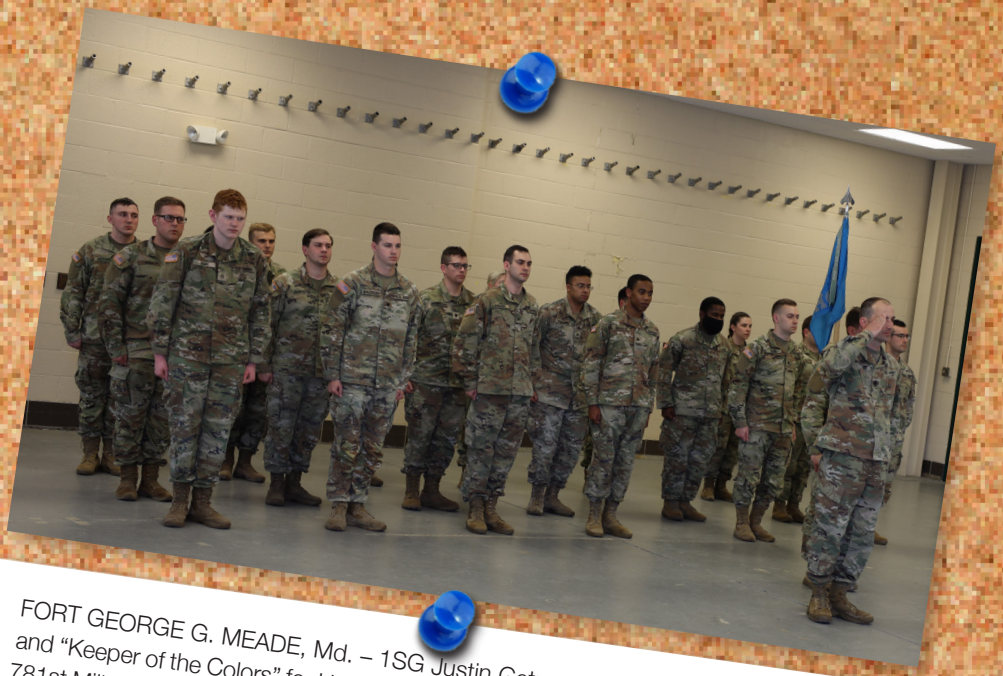
LAUREL, Md. – (Military Cyber Professionals Association HammerCon 2023) Soldiers and Army Civilians from the 780th Military Intelligence Brigade (Cyber) attended the Military Cyber Professionals Association (MCPA) HammerCon 2023 at Capitol Technology University on May 18 to promote the organization to attendees, including industry cybersecurity professionals, academia, and other service members, and discuss the life-changing opportunities of the U.S. Army Cyber branch.

ABERDEEN PROVING GROUND, Md. – (Aberdeen Proving Ground Armed Forces Week 2023) Soldiers from the 780th Military Intelligence Brigade partnered with Army Civilians from the U.S. Army Communications-Electronics Command (CECOM) Software Engineering Center (SEC) to talk to students, educators, and chaperones about the life-changing opportunities and possibilities that come with Army service at the Aberdeen Proving Ground Armed Forces Week, May 19. Aberdeen Proving Ground #beallyoucanbe #ArmyPossibilities.

ARLINGTON, Va. – Lt. Gen. Maria Barrett (left), commanding general, Army Cyber Command, Pfc. James Klein, a cyberspace operations specialist (17C), 781st Military Intelligence Battalion (Cyber), 780th MI Brigade, and retired Gen. Robert Brown, president and CEO of the Association of the United States Army, cut an Army birthday cake celebrating the U.S. Army's 248th birthday at the AUSA Hot Topic series on Army Cyber, General Gordon R. Sullivan Conference & Event Center, June 14. ■

FORT GEORGE G. MEADE, Md. – 1LT James Donahue (left), the commander of B Company (Immortals), 781st Military Intelligence Battalion (Cyber), during his change of command ceremony at the MG Baron DeKalb Army Reserve Center, April 12.

FORT GEORGE G. MEADE, Md. – SFC Angel Rodriguez (left) signifies his assumption of responsibility as the senior enlisted leader and "Keeper of the Colors" for B Company (Immortals), 781st Military Intelligence Battalion (Cyber), by accepting the company guidon from the B Company commander, CPT Allan Baily, in a change of responsibility ceremony at the MG Baron DeKalb Army Reserve Center, April 12.



FORT GEORGE G. MEADE, Md. – 1SG Justin Getzandanner, senior enlisted leader and "Keeper of the Colors" for Headquarters and Headquarters Company (Guardians), 781st Military Intelligence Battalion (Cyber), salutes CPT Natalie Herbert, the company commander, signifying the conclusion of his change of responsibility ceremony at the MG Baron DeKalb Army Reserve Center, April 12.

FORT GEORGE G. MEADE, Md. – CPT Allan Baily, the commander of the Headquarters and Headquarters Company (Hastati), 780th Military Intelligence Brigade (Cyber), informs COL Benjamin Sangster, the brigade commander, of the completion of his change of command ceremony, on the Parade Field, April 14.

FORT GEORGE G. MEADE, Md. – April 26, 2023, marks the 25th annual commemoration of Denim Day in the United States. The purpose for wearing denim on Denim Day is to outwardly express support for survivors of sexual assault and to visibly protest the myths and misconceptions surrounding sexual assault.

COLUMBIA, Md. – Soldiers from Headquarters and Headquarters Company (Hastati), 780th Military Intelligence Brigade (Cyber), had a Pickleball tournament at Dill Dinkers as part of the Brigade wellness program, April 28.

ARLINGTON, Va. – Army National Guard Soldiers from Task Force Echo VII, 125th Cyber Protection Battalion, currently assigned with the 780th Military Intelligence Brigade (Cyber) participated in a Wreath Laying Ceremony at Arlington National Cemetery, May 4. Formal ceremonies at Arlington often involve the laying of a wreath. These ceremonies typically take place at the Tomb of the Unknown Soldier, attended by ceremonial units from the uniformed services.

FORT GEORGE G. MEADE, Md. – 1SG Joel Aguilar, senior enlisted leader and "Keeper of the Colors" for Headquarters and Headquarters Company (Hastati), 780th Military Intelligence Brigade (Cyber), at his change of responsibility ceremony in the U.S. Army Reserve Center CPT John E. Smathers, May 5.

NATIONAL HARBOR, Md. – The 780th Military Intelligence Brigade (Cyber) Unit Ministry Team hosted a couples and family's event, May 5 at the Hyatt Place National Harbor. Chaplain (MAJ) Frances Igboeli, brigade chaplain, used The 7 Habits of Highly Effective Families for Military Families, as the curriculum to instruct seven Brigade couples attending the event.

FORT GEORGE G. MEADE, Md. – CPT Aaron Crapser, the commander of the Headquarters and Operations Company (Herculians), Task Force Praetorian, 780th Military Intelligence Brigade (Cyber), salutes MAJ Marissa Cina, the Task Force commander, signifying the completion of his change of command ceremony, on the Parade Field, May 11.

FORT GEORGE G. MEADE, Md. – C Company (Conquerors), 781st Military Intelligence Battalion (Cyber), Change of Command whereby CPT John Cloutier (right) relinquished his command to 1LT Andrew White (left) in a ceremony hosted by LTC Donald Sedivy, the battalion commander, on the Parade Field, May 15.

FORT GEORGE G. MEADE, Md. – CPT John McCarthy (left), the commander of Headquarters and Headquarters Company (Guardians), 781st Military Intelligence Battalion (Cyber), returns the company guidon to 1SG Justin Gatzandanner, the senior enlisted leader and “Keeper of the Colors”, during a change of command on Constitution Field, May 24.

TOCCOA, Ga. – The 782D Military Intelligence Battalion (Cyber) conducted a staff ride to Camp Toccoa, Georgia, to run Currahee Mountain as part of leadership development week. The team ran three miles up! And three miles down! At the historic training site of the 101st 506th Parachute Infantry Regiment during World War II. The staff ride was part of a three-day leadership development program put on for key leaders from the cyber teams in Georgia, Texas, and Hawaii. Cyber Legion, Silent Victory!

In Memoriam
SGT Ammel Rhyes M. Dooley
B/782d Military Intelligence Battalion

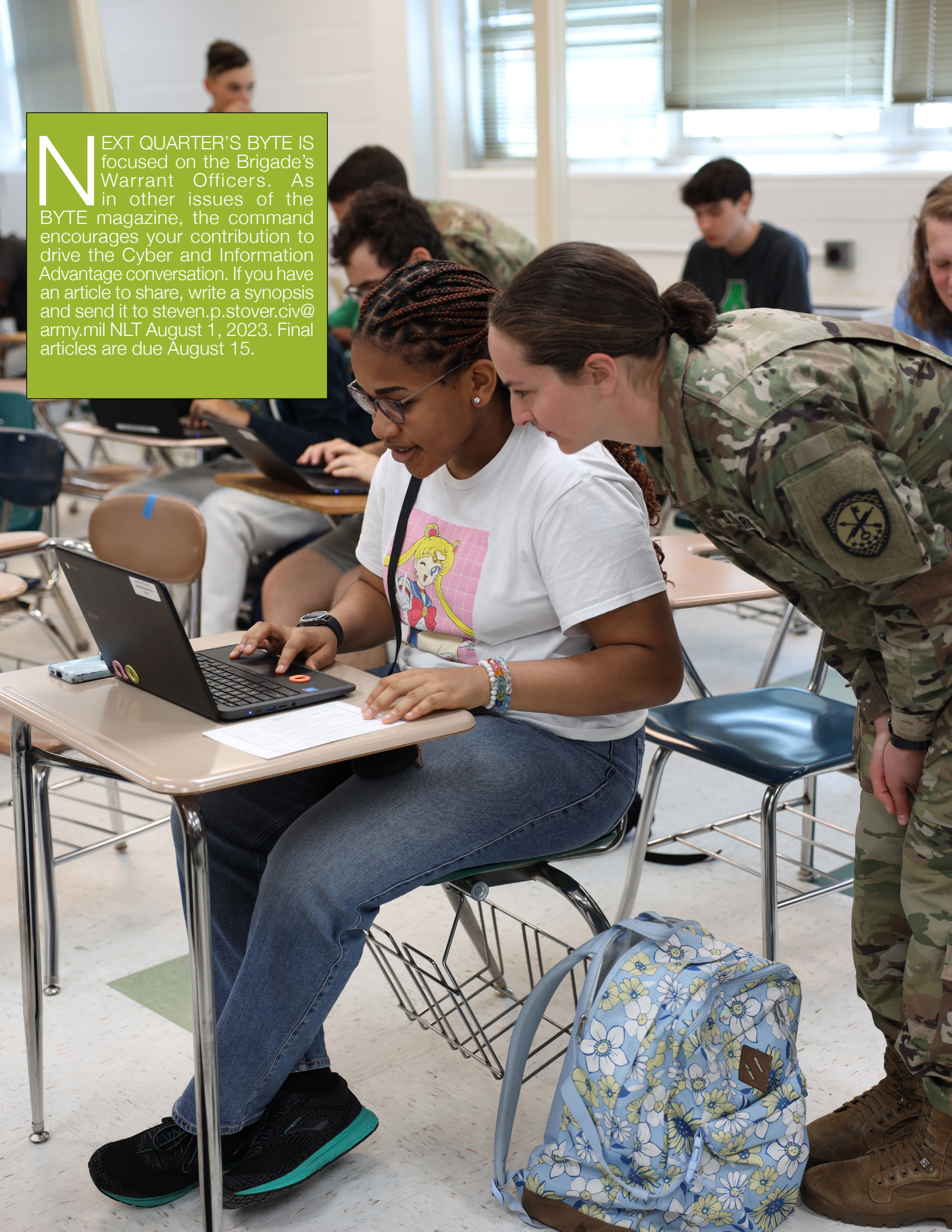
SGT Ammel Rhyes Michael Patrick Dooley was born on September 15th, 1998, in Fayetteville, NC to June and David Paul Dooley. He loved renovating his home, anything including combatives, rescuing animals, and outdoor adventures with his spouse, Jonathan.

SGT Dooley enlisted in the Army in 2018 from Fayetteville, NC. He attended Basic Combat Training at Fort Jackson, South Carolina, and Advanced Individual Training at Corry Station in Pensacola, Florida, before being assigned to Charlie Company, 781st Military Intelligence Battalion (Cyber) in 2019. Ammel worked as a Cryptologic Network Warfare Specialist from 2019 to 2021. He graduated Phase 2 of 17C Advanced Individual Training at Fort Gordon, Georgia in 2021 and was assigned to Bravo Company 782d Military Intelligence Battalion (Cyber) at Fort Gordon, Georgia, where he worked as a Cyber Operations Specialist on 103 Combat Mission Team. From 2021 to 2023, he served as a Priority Lead and a Digital Network Exploitation Analyst, finally achieving the certification of Senior in April 2023.

During his service, SGT Dooley was awarded the Meritorious Service Medal, Army Achievement Medal with one oak leaf cluster, Army Good Conduct Medal, National Defense Service Medal, and the Army Service Ribbon. His training includes Basic Leaders Course, Joint Cyber Analysis Course, Combat Lifesaver's Course, and earned a SANS professional certificate in Behavioral Malware Analysis.

SGT Dooley is survived by his husband, Jonathan, his beloved siblings Angela, Stephen, Shi-Annia, Kelson, Ambrose, Nordac, Gabrille, Jaydin, Colin, Aibhilin, and his parents, June and David Paul Dooley. ■


DOOLEY
UTAH
AIRBORNE
DOOLEY



NEXT QUARTER'S BYTE IS focused on the Brigade's Warrant Officers. As in other issues of the BYTE magazine, the command encourages your contribution to drive the Cyber and Information Advantage conversation. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT August 1, 2023. Final articles are due August 15.