


780th MILITARY INTELLIGENCE BRIGADE (CYBER)

# THE BYTE

Vol. 12, Issue 2



Where We've Been,  
Where We're Going!





COL Benjamin Sangster  
Commander  
CSM Joseph Daniel  
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](mailto:steven.p.stover.civ@army.mil), or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.



**Evolving the 781st and the CNMF:  
Supporting a Sub-unified Command**  
LTC Donald Sedivy, 781st MI BN (Cyber)

**JTF-4 Force Structure Pilot: Identifying OCO  
Maneuver Units**

LTC Donald Sedivy, 781st MI BN (Cyber)

**Updating Generational Perspective to Match the  
Evolving Online Environment**

1LT Nicole Moore, 781st MI BN (Cyber)

**Cyber Legion Vision**

LTC Kirklin Kudrna and CSM Jamie Stargell, 782d MI BN (Cyber)

**Notes on the Role of the Commissioned Officer  
in Cyber**

1LT Thomas Bordeaux, 782d MI BN (Cyber)

**Shaping Future Leadership in the Cyber Mission  
Force Through Lessons Learned**

1LT Michael Mercier, 782d MI BN (Cyber)

**Cyber Officers: Students for Life**

1LT Jack Summers, D CO, 782d MI BN (Cyber)

**Hawaiian Horizons: Junior Officers Lead New Wave  
of Capability Development**

1LT Reed Burton, Det Hawaii, 782d MI BN (Cyber)

**A balance in technical and professional Officer  
Development**

CPT Laura Adams, Det Texas, 782d MI BN (Cyber)

**Task Force Future**

MAJ Ben Liles and MAJ Michael Krogh, TF – Praetorian

**Cyber Leader's Conference at West Point**

MAJ Mark Klink, TF – Praetorian

**AvengerCon VIII – Army Cyber's homegrown hacker  
con returns**

780th MI BDE (Cyber)

**Vanguard "When Others Cannot" Change of  
Responsibility**

780th MI BDE (Cyber)

1

5

7

9

10

11

12

13

15

18

19

21

26



**Praetorians honor one departing senior enlisted leader and welcome another**  
780th MI BDE (Cyber)

**Corkboard**

**Task Force Praetorian Unit History**

**Task Force Praetorian Operational Support Element Change of Command**  
780th MI BDE (Cyber)



**On the Cover**

**Apex Flex!**

**FORT EISENHOWER, Ga.** – Soldiers from A Company (Apex), 11th Cyber Battalion, completed the Marine Corps obstacle course, February 9. Apex Soldiers are committed to staying ready, while building esprit de corps; and completing the challenge together. Train Hard, Fight Hard, Win Easy! Leviathan Strong! (U.S. Army photos by 1LT Angeline Tritschler)

28

31

51

52

**R**ecently COL Ben Sangster, Praetorian 6 and the seventh commander of the 780th Military Intelligence Brigade (Cyber), stated his theme for this edition of The BYTE magazine, “Where we’ve been and where we’re going.”



He told the commanders it was an opportunity to tell their commands about the recent changes, including the alignment of the 781st Military Intelligence Battalion (Cyber), the Vanguard, under the operational command of the Cyber National mission Force in October 2023; the vision of the command team of the 782d MI Battalion (Cyber), Cyber Legion; the recent signing of an MOU (memorandum of understanding) between U.S. Army Intelligence & Security Command and U.S. Army Cyber Command whereby the 780th MI Brigade (Cyber) provides the 11th Cyber Battalion brigade commander signature authority for administrative support actions, as well as S1 (personnel) and S3 (operations) support; the way ahead for Task Force Praetorian, an operational support element, and newest Praetorian organization; and the end of mission for Task Force Echo after eight iterations.

Additionally, if you haven’t heard, the brigade is standing up its own Praetorian competitive cyber team with the target of competing in remote or in-person events. The point of contact is MAJ Mark Klink, mark.c.klink.mil@army.mil. The commander’s intent is for this competitive cyber team to compete in an event before the summer’s end.

Furthermore, look for a forthcoming Brigade TASKORD discussing time trials for this year’s Brigade Army Ten-Miler team. This year is the 40th ATM and the brigade looks to build upon the success of the previous year’s team, which barely missed out on a top three team finish; and 1LT Kristen Gray, a 17A, and a member of the Howard County Striders Racing Team, placed 3rd in the military female category of the 39th Army Ten-Miler race.

Finally, congratulations to the Soldiers from Detachment Texas (Cyber Rangers), 782d MI Battalion (Cyber), who recently represented the 780th MI Brigade (Cyber) and finished 22nd out of 66 military (including ROTC) teams – 23rd out of 74 overall, in the Bataan Memorial Death March 2024, Team Military Division, March 16.

Praetorians! Strength and Honor  
v/r,  
Steve Stover  
Public Affairs Officer  
780th MI Brigade (Cyber)  
Editor, The BYTE





# Evolving the 781st and the CNMF: Supporting a Sub-unified Command

By LTC Donald E. Sedivy, commander, 781st Military Intelligence Battalion (Cyber)



THE CYBER NATIONAL MISSION FORCE (CNMF) was created in January 2014 to defend the Nation in cyberspace and has subsequently undergone substantial evolution and growth during the last decade. Among the most recent and significant of these evolutions was the designation of the CNMF as a subordinate unified command in December 2022 and the subsequent alignment of the entire 781st Military Intelligence Battalion (Cyber) under its operational command in October 2023. The 781st, true to its name as the Vanguard, has led the way in embracing its new command relationship and with it the new responsibilities and opportunities to mature the talent management, training, and operating efficiency of the Nation's preeminent cyber force. By anticipating changes, implementing tailored programs designed to grow talent and readiness, and collaborating with the CNMF staff, the 781st is poised to lead the CNMF's continued evolution to enable elite operational support.

## The Past is Prologue: Leaning into Coming Changes

Combatant Commands (CCMDs) establish subordinate unified commands (sub-unified commands) when authorized by the Secretary of Defense for the purposes of executing operations continually in either a geographic area or on a functional basis. In the specific case of the CNMF, CYBERCOM established the CNMF as a functional sub-unified command in "recognition of its enduring mission to combat foreign malicious cyber actors, reflecting its on-going success in support of national priorities and formalizing its organizational structure". Upon sub-unification, prominent among the topics of discussion for maturing the CNMF was the command relationships

that it should have with the various service units that provisioned its NMTs and NSTs (National Mission Teams / National Support Teams). While those discussions occurred at the service component level starting at the beginning of 2023 and persisted throughout the end of FY23, the 781st, newly reorganized to only have CNMF-aligned elements assigned to it with the stand-up of Task Force Praetorian (TF-P), leaned into generating initiatives that would support increasing the readiness of all joint forces assigned to the CNMF as listed in Figure 1.

The first of these initiatives was the implementation of Tradecraft Academy. Foremost among the 781st's responsibilities as a force-provider to the CNMF is provisioning work-role trained and certified individuals at the appropriate skill level as dictated by the Deputy Secretary of Defense readiness memo. The 781st created Tradecraft Academy in March 2023 to accelerate the progression of analysts (Digital Network Exploitation Analysts (DNEAs), Target Digital Network Analysts (TDNAs), Target Analyst Reports (TARs), and Language Analysts (LAs)). Originally run as a pilot iteration with CNMF JTF-1 (Joint Task Force) to determine its feasibility, the CNMF established Tradecraft Academy as a formal program in July 2023. The program stipulates that every quarter a designated JTF dedicates a week where it allocates experienced senior analysts to teach aspirant senior analysts on tasks and skills associated with their respective senior Job Qualification Record (JQR) with content provided and curated by the 781st. To date, the CNMF has executed two additional iterations of Tradecraft Academy that has generated a marked decrease in the time required to generate senior qualified analysts and an increase in the total number of senior analysts.

As a complement to Tradecraft Academy,

781st established its Structured On-the-Job Training (SOJT) initiative in the Spring of 2023. SOJT tasked subject-matter experts across the battalion to generate vetted training content for each of its supported work roles as well as guides for the overarching topics of analyst fundamentals, policy fundamentals, operational planning, and the intelligence cycle to allow first line supervisors to conduct training with their Soldiers and Civilians at the lowest level without the overhead of having to generate their own content. The first SOJT materials were generated in July 2023 in a combination of guides posted on high-side repositories as well as PCTE-hosted content for the exploitation analyst (EA) and operator work roles. The content is designed to be living documents that are continuously refined and updated as new knowledge and gaps are identified. To assess the effectiveness of this program, 781st will collect metrics the amount of time reduced to prepare individual training and the amount of individual training that Soldiers complete.

To continue to improve proficiency and readiness at the individual level, the 781st also maintains an Adjunct Faculty (ADFAC) program that while common across the 780th is not widely implemented across the other services supporting the CNMF. 781st executes a yearly review of National Cryptologic University (NCU) course shortfalls during its May planning summit that drives ADFAC recruiting and training in a proactive manner to fill the requirement for CYBERCOM pipeline course. To date, 781st maintains 23 ADFAC certified personnel with projections to increase to 32 ADFAC certified personnel in the next quarter to support slotting for critical NCU pipeline courses.

Advancing past the individual level, the 781st has partnered with the CNMF



J7 for the execution of JTF Collective Training Events (CTEs) since they were first implemented in 2021 assisting with scenario and Persistent Cyber Training Environment (PCTE) content development, range support, and assessors for the event. Most recently, the 781st provided support to JTF-2 and JTF-3's CTEs executed April and November 2023 respectively with lead-up events throughout 2023 resulting in those JTFs recertifying their proficiency against their JMETs established by CNMF.

Lastly, beyond technical and tactical training and the individual and collective level, 781st implemented its Vanguard Academy in June 2023 to equip its small-unit leaders with practical leadership skills and techniques to navigate the unique operating environment of the CNMF. Executed in separate versions for both junior NCOs (E5-E6) and junior officers (O1-O3), Vanguard Academy provides instructional blocks on effective communication, training management, relationship building, and time management while providing an open forum for senior leaders offer lessons learned and mentorship opportunities to empower junior leaders in a proactive manner. While quantitative metrics for measuring leadership training effectiveness can be elusive, qualitative metrics the 781st uses to assess this program are increased mentorship interactions, junior leader empowerment, and leader trust which inform the quantitative metric of retention.

### Writing the Future: Grow Talent and Accelerate Force Readiness

Reflecting upon my 19 years of service and observing units undergoing change, those units that have been proactive in implementing change rather than reactive tend to have first-mover advantage and set a more positive tone than those trying to cling to the past. 781st started each of forementioned initiatives prior to the formal declaration of the CNMF's operational control over it in October 2023 and have allowed the 781st to set the foundation for what support to a cyber sub-unified command can be. The advantage to this proactive approach is

that once operational control officially transferred to the CNMF and our current initiatives were presented to the CNMF commander, the 781st was instructed to continue to proceed with its ongoing initiatives as we had been informing the CNMF of our plans throughout the implementation. Thus, the transfer of operational control became an in-stride event rather than a disruptive one for the 781st. We were already executing the commander's intent and did not have to go through a massive staff churn and resulting shock to the force to re-adjust when the command relationship changed.

With the assignment of a new CNMF Commander in January 2024, Maj. Gen. Lorna Mahlock, United States Marine Corps, set forth a vision to mature the CNMF as a sub-unified command with priorities for growing CNMF talent and accelerating force readiness for her service component headquarters. In the 781st's initial commander's estimate to her, illustrated in Figures 2 and 3, 781st articulated how its ongoing initiatives mapped to her priorities and where the opportunity space exists for further development. In addition to continuing with Vanguard Academy, 781st identified converting three 131A billets to 13A CPT billets to increase Fires Planner support, accelerating civilian hiring through clearly articulated 780 MI Brigade policy and SOPs (standard operating procedures), offering enhanced training opportunities, and interviewing BOLC 2LTs/1LTs as initiatives to grow CNMF talent. To accelerate force readiness at the individual, 781st plans to build upon its already existing Tradecraft Academy and SOJT initiatives with the implementation of a 14-week Cyber Crash Course for Soldiers and Civilians awaiting NSA indoctrination that will sharpen and baseline all analysts and operator aspirants in the fundamental principles of the domain coupled with practical exercises to reinforce their knowledge. A Company, 781st is currently championing the Cyber Crash Course with expected implementation in March 2024. To accelerate force readiness at the collectively level, the 781st is proposing the CNMF implement a more robust series of

lead-up events in the form of INTELEXs, OPEXs, and PLANEXs (exercises) executed at the sub-element, Joint Mission Team, Operator Element, and staff levels in addition to a Mission Rehearsal Exercise (MRE) prior to the execution of its JTF CTEs in a manner similar to how Operational Readiness Assessments (ORAs) are executed for CMTs and CSTs.

### Conclusion

The establishment of the CNMF as a sub-unified command in December 2022 was a seminal moment in its history that indicated that the CNMF's mission is enduring and requires an appropriate maturation of the command and its relationship with its subordinate elements. As one of CNMF's newest operationally controlled elements, the 781st has leaned into supporting the command through its Tradecraft Academy, SOJT, ADFAC, CTE support, and Vanguard Academy initiatives prior to formal alignment. By communicating early and often with the purpose and value of these initiatives, 781st completed the transition under the CNMF in a seamless manner that has allowed it to begin championing new initiatives for growing CNMF talent and accelerating force readiness that will assist in evolving the command to new heights *when others cannot*.

### References:

- <sup>1</sup>"The Evolution of Cyber: Newest Subordinate Unified Command is Nation's Joint Cyber Force", CNMF Public Affairs, December 19, 2022, <https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cyber/>
- <sup>2</sup>Ibid
- <sup>3</sup>"Combatant Command (CCMD) Command and Control Organizational Options", Deployable Training Division, Joint Staff J7, June 30, 2022. [https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/ccmd\\_c2orgops.pdf?ver=nioA3r8g4gYD3n4DuHACNg%3D%3D](https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/ccmd_c2orgops.pdf?ver=nioA3r8g4gYD3n4DuHACNg%3D%3D)
- <sup>4</sup>"The Evolution of Cyber: Newest Subordinate Unified Command is Nation's Joint Cyber Force", CNMF Public Affairs, December 19, 2022, <https://www.cybercom.mil/Media/News/Article/3250075/the-evolution-of-cyber-newest-subordinate-unified-command-is-nations-joint-cyber/>
- <sup>5</sup>"Cyber National Mission Team and Cyber National Support Team Standardized Readiness", Deputy Secretary of Defense Memorandum, May 27, 2021. ■



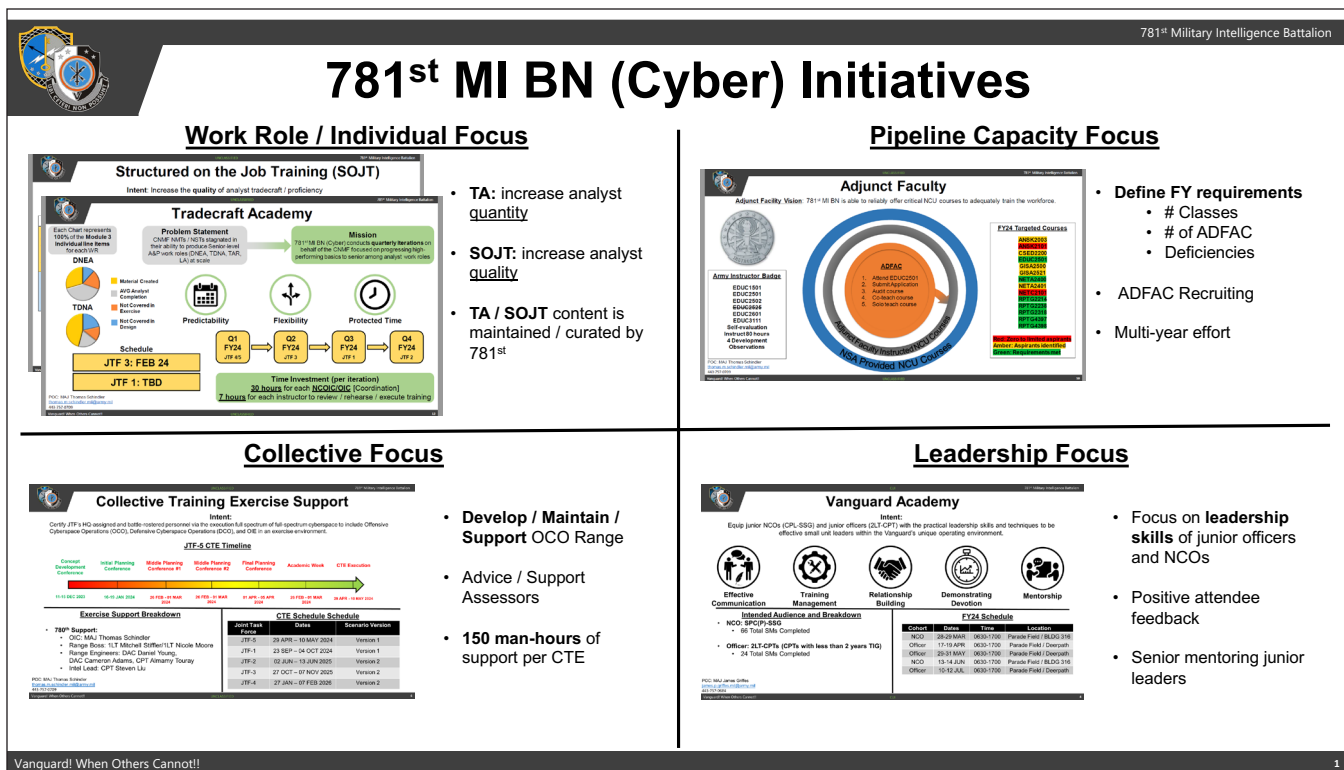


Figure 1. 781st MI BN (CYBER) Initiatives

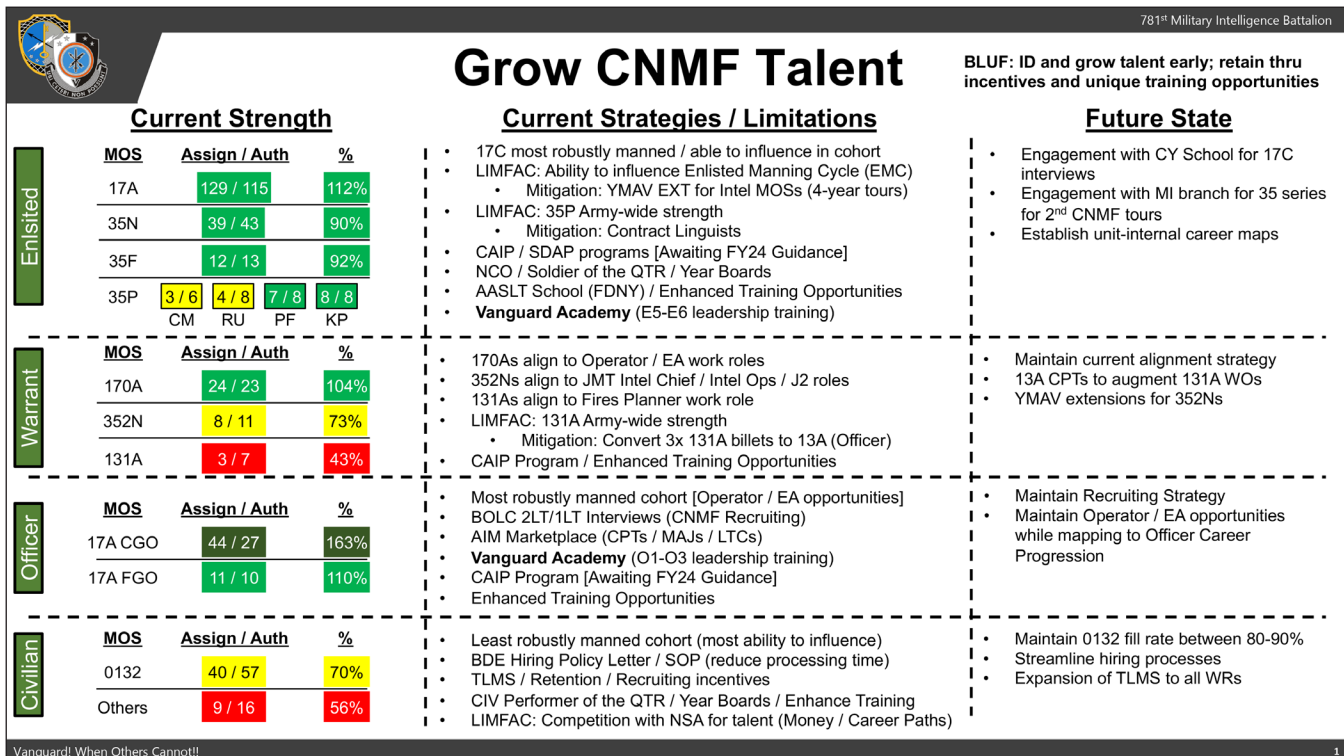


Figure 2. Grow CNMF Talent



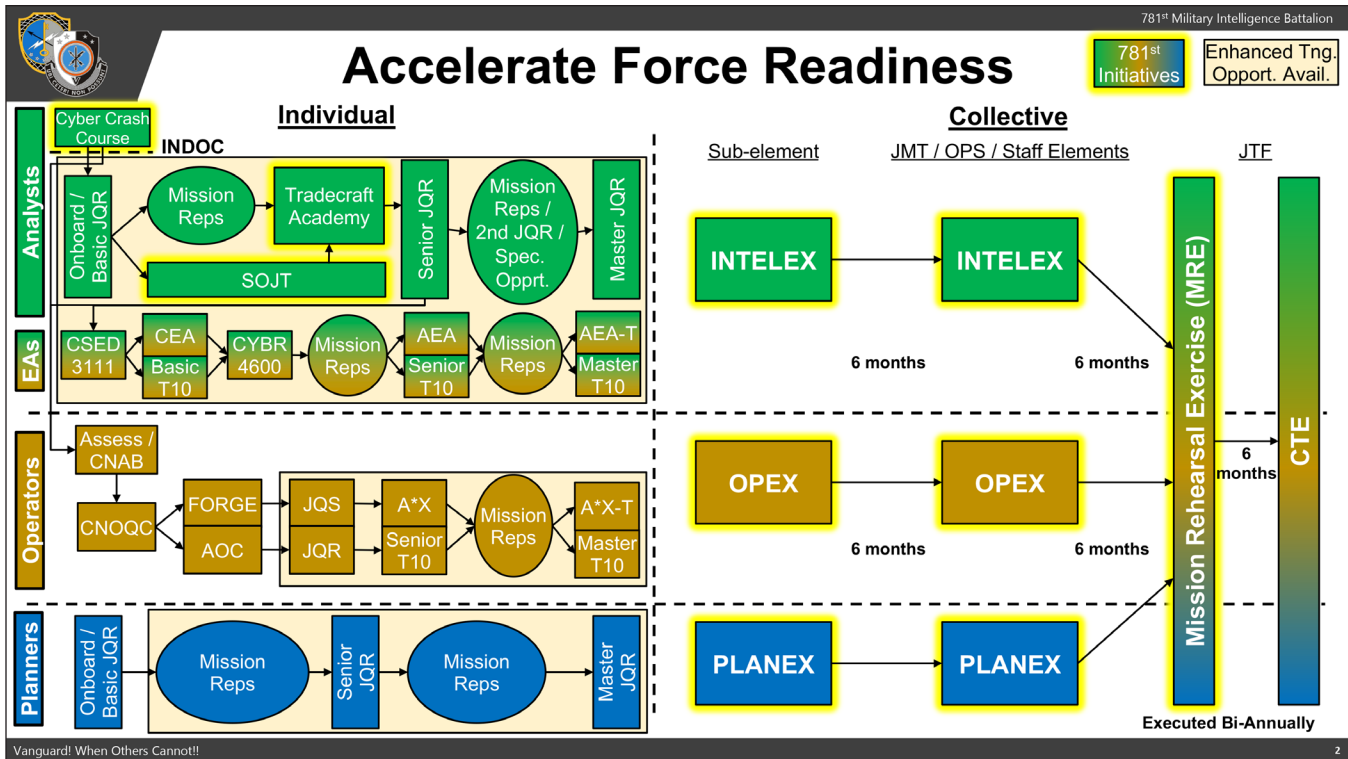


Figure 3. Accelerate Force Readiness







# JTF-4 Force Structure Pilot: Identifying OCO Maneuver Units

By LTC Donald E. Sedivy, commander, 781st Military Intelligence Battalion (Cyber)

SINCE THE DEPUTY SECRETARY OF DEFENSE (SECDEF) AND CYBERCOM defined the structure and readiness requirements associated with National Mission Teams (NMTs) and National Support Teams (NSTs) in 2021, the Cyber National Mission Force has continued to develop how to execute offensive cyberspace operations in defense of the Nation. Currently, the CNMF assigns NMTs and NSTs to Joint Task Forces (JTFs) with the JTFs subsequently task organizing them into Joint Mission Teams (JMTs), Operation Elements, and JTF staff elements to support mission requirements. The exact composition of JMTs across the each JTFs has varied widely across the last several years with JTFs implementing their own structure based on their unique demands. While the ability task-organize is an inherent and essential part of any command, the further that a commander has to task organize their forces from what a service presents to them, the more friction and ambiguity is introduced into the implementation of the force. As currently implemented, NMTs and NSTs are functionally disintegrated upon presentation to the CNMF making it difficult to articulate a JTF's true capacity to execute operations while also creating problems with unit identity and cohesion between the individual and JTF level. To remedy this, 781st Military Intelligence Battalion (Cyber) in partnership with CNMF JTF-4 is implementing a pilot to determine a standardized structure for a JMT consisting of three "Exploitation Elements" derived from the billets provided in a single NMT and NST (minus developer element structure). Defining a JMT in this manner also generates additional supporting functions provisioned under the team construct that now operating under a JTF structure.

## NMT / NST Overview

The left side of Figure 1 depicts the Deputy SECDEF specified NMT and NST structure. NMTs consist of an intelligence element, a support element, and five mission elements and NSTs are similarly structured with an intelligence element, support element, and a developer element in lieu of mission elements. The 780th MI Brigade (Cyber) has consolidated developer elements across NSTs and CSTs into Capability Solution Development (CSD) detachments across its footprint and are functionally not associated with their teams. Moreover, with the official establishment of the Operational Support Element (colloquially referred to as Task Force Praetorian (TF-P)) on March 1, 2024, as its own stand-alone Unit Identification Code (UIC), the 780th has formally reorganized its developer force structure under a consolidated headquarters.

## Overview of Force Structure Pilot Model and Metrics

The right side of Figure 2 depicts the JMT pilot structure. The pilot proposes the creation of a JMT with three 15-person "Exploitation Elements" (ExEs) by reallocating billets derived from the standard intelligence element and mission element models. Additionally, the pilot also creates an operator element, linguist support cell, and targeting cell as JTF-level assets to support the maneuver of ExEs along with standard JTF leadership and staff functions. The ExE intends to capture the offensive cyberspace operations (OCO) fundamental maneuver unit.

The key innovation of the ExE is the inclusion of exploitation analysts (EAs) with the rest of the intelligence element analysts (hence "exploitation element"). EAs have always had a dual role to both drive the cyberspace maneuver of operators while feeding the requirements

of the intelligence element to facilitate the SIGDEV (Signals Development) necessary to drive cyberspace operations. A potential flaw of having EAs outside the intelligence element is that they can view the SIGDEV work so critical to driving operations as someone else's problem. Embedding the EAs with analysts forces them to drive SIGDEV while affording them the opportunity to mentor more junior analysts and provide operational context to their work. To support the execution of cyberspace operations, EAs will pair up operators from the JTF's operator element and a JMT-provided Mission Commander (MC). Planning for the pilot considered directly embedding operators within the ExE but did not include operators in this iteration to assess the training benefits of a single consolidated operator element at the JTF level.

Examining the rest pilot structure, the pilot ExE reduces the number of Digital Network Exploitation Analysts (DNEAs), Target Digital Network Analysts (TDNAs), Target Analyst Reporters (TARs) and Language Analysts (LAs) from the number associated with a NMT standard intelligence element but results in a JMT with three ExEs that contain a strength equivalent to the combined strength of an NMT and NST intelligence element (45 personnel). This structure's advantage is that a JMT lead now has standardized subordinate elements that he can assign missions and tasks to instead of tasking individual members. Moreover, to improve readiness and predictability at the collective level, the pilot will designate one ExE in a training status with the other two in a mission status to allow for a training cycle above the individual level.

The creation of the ExE structure also spawns the creation of two additional structures in addition to the operator element: the linguist support cell (LSC) and targeting cell. The pilot designs ExEs

with a single LA that the pilot envisions as an experienced linguist who can cultivate deep target knowledge and context with the rest of the ExE analysts. The LSC consolidates the remainder of the presented LAs intended to can centrally manage the JTF's translation requirements to the best qualified analyst for the task while facilitating training and mentorship for junior LAs in a more systemic manner. The targeting cell, typically task organized at the JTF level within the CNMF, centralizes fires planning, targeting analysis, and all-source functions to support all JMT and JTF requirements. LA and Fires functions are low-density functions in cyberspace operations can be more efficiently executed at the JTF echelon versus the team echelon resulting in a more sustainable readiness model for the CNMF. The remaining NMT and NST support element force structure and functions have already been repurposed

into JTF leadership and staff functions and are outside the scope of this pilot.

JTF-4 will begin the force structure pilot in March 2023 and assess the structure's effectiveness at the 60-day mark for continued use and refinement. Among the metrics in use for the pilot are time for target development, span of control per leader, number of operations executed, analyst training progression and skills development, and operational flexibility. Additionally, the creation of smaller maneuver units generates the opportunity to empower junior leaders with responsibility and latitude that feeds secondary metrics associated with career progression and mentorship opportunities.

Conclusion

The CNMF has been at the forefront of innovating cyberspace operations since its inception in 2014. This force structure pilot is designed to take the

functions and roles inherent in NMTs and NSTs and map them to an operational construct more closely aligned with how the CNMF is employing its forces that maximizes operational flexibility while porting low-density functions to the JTF level to optimize readiness and reduce the overhead cost of those low-density functions. The results of this pilot will provide the basis for continued analysis on a fully updated CNMF force structure that informs CYBERCOM 2.0 and NDAA updates in the forthcoming years.

References:

<sup>1</sup>"Cyber National Mission Team and Cyber National Support Team Standardized Readiness", Deputy Secretary of Defense Memorandum, May 27, 2021. ■

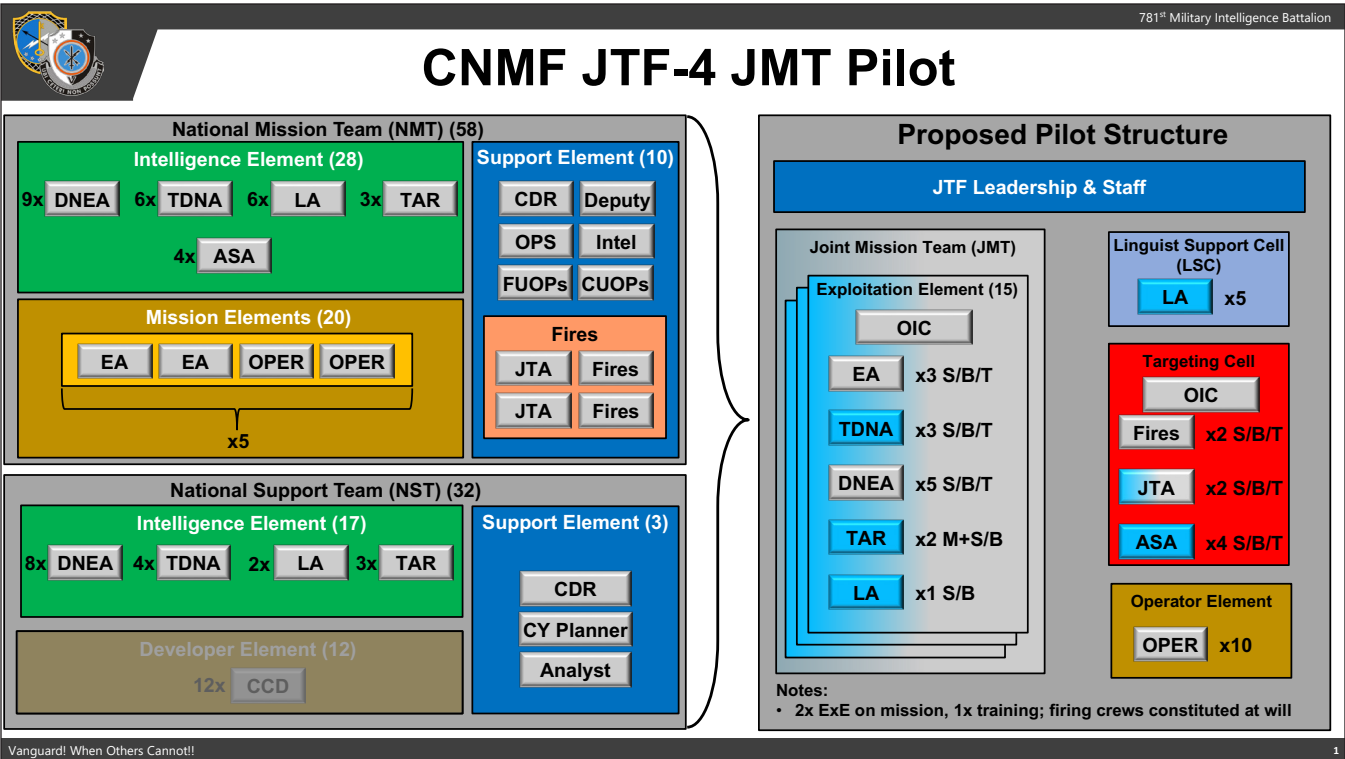


Figure 1. CNMF JTF-4 JMT Pilot





# Updating Generational Perspective to Match the Evolving Online Environment

By 1LT Nicole Moore, Assistant S3 (operations), 781st Military Intelligence Battalion (Cyber)

**A**S SOMEONE BORN AT THE TURN OF THE 21ST CENTURY, I still remember the periodic Yellow Pages dropped at the doorstep as a young child. I also remember seeing advertisements for the first smartphone with touchscreen capability to enter the mainstream and chattering amazedly with friends about it on the bus ride home from school. Another time shortly after, I was in the grocery store and saw a man stand out, seemingly carrying on a full conversation with himself, only to see an earpiece as he turned and learn that Bluetooth was the next big thing.

When I was growing up, very few kids had smartphones. I received a prepaid flip phone for emergencies towards the end of middle school. Today, 95 percent of teens between 13 and 17 have access to a smartphone, essentially a miniature computer, within arm's reach constantly<sup>1</sup>. No previous generation has grown up in that kind of environment, one with every answer, perspective, and potential bias just a few taps away. Adults who were introduced to connected devices later in life are fully integrated now, with average daily recreational screen time for adults 16-64 being 6.6 hours per day<sup>2</sup>. This technology, currently progressing in leaps and bounds, presents tools that are beneficial or harmful depending on whose hands they lie in. It allows for disinformation and social influence to spread on an unprecedented scale. It's easier to deceive, but also easier to detect. Individuals need to develop habits centered around intentional awareness to protect the outputs they generate in the online environment and protect themselves from the inputs they receive from this same environment. Outputs of an individual include online personas, social media accounts, and open-source perception of online activity. Inputs are any online interactions an individual has,

known or unknown to them, which can generate various effects on those individuals. Examples of inputs would be targeted marketing, phishing attempts, mental health effects, and social engineering.

When I first arrived at the 781st I was afforded the opportunity to attend a SANS course of my choosing. Of all the possible options, a newly published course stood out to me, SEC 497: Practical OSINT (Open-Source Intelligence). I figured this was a unique opportunity to pursue something I was genuinely curious about which hadn't yet made its way into my training curriculum. The tools I learned about in this course offered a brief glimpse into what is currently possible and within reach for anyone with basic internet access and the ability to create a free account, or at most, spend a few dollars. Moreover, it showed me what will be readily accessible to the average consumer with no technical background in only a few short years, as OSINT tools are frequently consolidated and updated. Below are just a few examples pulled from this vast expanse of double-edged tools that can be used for virtuous or nefarious purposes.

## **This-person-does-not-exist.com**

Cost: Free

This website generates images of fake people. Initially, it could be used to create fake social media accounts. Today, these can be used in normal digital correspondence to fool humans, but it is much more difficult to subvert social media account creation software with these images. As seen in the photos, the position of the eyes in this program is always aligned perfectly horizontally. However, face merging programs such as Face Swapper and Icons 8 can combine a

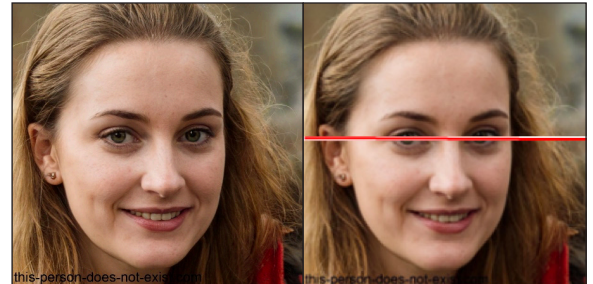


photo of a real person and an artificially generated person to create a more realistic decoy, one that can potentially be used in sock puppet accounts.

## **Self-Hosted VPNs**

Cost: \$3.80/month VM, ~\$3/month VPN

For increased anonymity and protection, one could opt to host their own VPN server for around \$7 per month. You have the option of using a free VPN. However, as a rule, if something is free you are likely the product, and any data that passes through these free services is collected and potentially used for the benefit of the company. The idea is to rent a VM through a service such as Amazon Web Services (AWS) or Microsoft Azure, then use the VPN through a key-protected resource group.

## **Wayback Machine**

Cost: Free

This website allows you to plug in the URL of any website to see screenshots of past versions of the page. If a site is taken down but you want to see the content that it hosted, this tool can be helpful. The only stipulation is that the site in question must allow or have allowed crawlers (internet bots used by search engines for the purpose of indexing content). This is useful if you are trying to see the original content of a news site, or potentially view original blog posts of a person of interest that have since been deleted.

### **AWS Rekognition**

Cost: Free for first year

Rekognition is an image and video analysis tool that can compare content and determine similarities, analyze logos and text, and detect real faces, among other things. For example, you can use this if you want to prove or disprove the identity of an individual by comparing multiple photos and seeing if they come back as matching or not.

### **OpenAI Whisper**

Cost: \$.006 per minute

Whisper is an automatic speech recognition (ASR) software that takes multilingual data from an audio file and translates it into human-readable words and sentences. This allows those who may not speak a certain language to obtain a translation of content and form an impartial perspective of the message before it is translated and interpreted by sources that may be biased.

These examples show how easy it is to be misguided online, especially with tools that are so readily available. However, just as easily as they can be used to cause harm, they can be used to protect or uncover truths about what is being presented and how one is presenting themselves. It would be prudent to make the public more aware of the abilities and limitations of their digital world, starting early and following up as this sea of capabilities grows and changes over time.

Similar to how flossing and brushing is now common practice for all ages to retain proper dental hygiene and longevity, I see something like “cyber hygiene” becoming a standard part of early education that is updated and retaught as the online environment evolves. An example of this already becoming reality would be a curriculum currently being taught to Swedish grade schoolers. After launching a study in 2017 assessing the quality of news stories ending up in front of students, the Swedish government discovered a need to develop a media credibility program held in the same regard as basic literacy and arithmetic<sup>3</sup>. This program implemented on a larger scale would give students a head start in approaching situations where

they may be taken advantage of online from lack of understanding. It would encourage critical thinking in situations like viewing different articles covering the same issues and comparing tone and biases observed. Students could also be shown the permanence of content posted online, as well as the revisable nature of online media.

The U.S. military has resolved to hold itself to a higher standard and set a positive example in society; that standard should extend to the cyber domain, affirming this concept of cyber hygiene. Cyber personnel are effective in their daily missions, but more emphasis should be placed on force protection of Soldiers apart from their mission requirements and their families. Examples of this could be sending home cyber awareness programs, distributing checklists for safe online practices that are categorized based on skill level of the user, and providing cyber awareness training and introductory computer skills and technical courses. These would be free resources that are available to all who are willing to learn. Soldiers should be encouraged to ensure their loved ones are taking the same precautions they would online, such as using a VPN and creating robust passwords. Essentially, Soldiers should be champions of the common practices they likely implement automatically in their daily lives for others around them.

Furthermore, effective national defense is kindled first from within our borders starting at the independent level. All citizens must be empowered to know what threats they face and how to effectively protect themselves. Preparing the public for cyber threats and online authenticity would mean setting them up for success early with previously mentioned techniques implemented on a larger scale. It would mean starting in the foundational years in public and private education institutes and continuously building upon instruction with lessons learned, real-world examples, and practical guidance as students progress. For those out of grade school, more emphasis should be placed on conscious use, understanding how personal data is exploited, and identifying protective steps for personal devices. The

technology industry should be encouraged to take consumer protection seriously, with basic cyber awareness training becoming standard during the initial bootup of a new computer, while more tailored training can come with software programs downloaded. Internet providers can similarly contribute. For example, in the same way taking drivers education can lower your auto insurance premium, an internet safety course can be incentivized with a discounted monthly bill. Ignorance isn't a valid defense on any stage, and these steps would help develop necessary skills in the digitally enforced world we are transitioning to.

It is our responsibility as conscious, intentional members of our Nation to ensure current and future generation are better equipped to approach the online environment with a healthy dose of realism and awareness of potentially invalid information. It's in this responsibility that we prepare others for success in navigating the uplinked world that the majority of their lives will surely center around. Ideally, early and continuing education, both formal and informal, will help all of us to become fortified with the appropriate skills and knowledge of how to protect ourselves and present as our most authentic selves in the evolving online environment.

### **References:**

<sup>1</sup> [https://www.washingtonpost.com/](https://www.washingtonpost.com/technology/2023/what-age-kid-phone/)

[technology/2023/what-age-kid-phone/](https://www.washingtonpost.com/technology/2023/what-age-kid-phone/)

<sup>2</sup> <https://www.health.com/>

[screen-time-limits-adults-8413940](https://www.health.com/screen-time-limits-adults-8413940)

<sup>3</sup> <https://www.thelocal.se/20170313/>

[swedish-kids-to-learn-computer-coding-and-how-to-spot-fake-news-in-primary-school](https://www.thelocal.se/20170313/swedish-kids-to-learn-computer-coding-and-how-to-spot-fake-news-in-primary-school) ■





# Cyber Legion Vision

By LTC Kirklin Kudrna, commander, 782d MI BN (Cyber), and  
CSM Jamie Stargell, senior enlisted leader, 782d MI BN (Cyber)

**T**HE COVID-19 PANDEMIC necessitated unprecedented adaptiveness and flexibility, requiring new communications, procedures, and battle rhythm norms. We are grateful for the leadership our predecessors, indeed of all Legionaries, who steered the Battalion through those difficult times with resilience and professionalism. However, the organizational effects of COVID still can be felt years after the resumption of normal operations.

A core competency of the military profession is the process of determining the progress and effectiveness of our actions and decisions. Assessment helps us to identify gaps, measure performance, and improve outcomes. As CSM Stargell and I transitioned into the Battalion, we took the opportunity to assess the Battalion's course. To achieve a comprehensive and objective view we held a long-range planning meeting with team, company, and detachment (Officer, Warrant, Civilian, and NCO) leaders from Georgia, Texas, and Hawaii. With their expertise and experience we collectively identified key areas for improvement. Our assessment is the basis for the 782d's Battalion vision:

*782d delivers high-performing people and impactful results through sound fundamentals and persistent innovation.*

A good vision drives behavior and change. Our vision has the following goals:

**Goal 1:** Reinforce the fundamentals. This goal is to improve the way we do Army business and we have already moved out. We started by reinforcing basic Army processes and standards, revising the Legion's business rules, establishing timeliness in civilian and military awards and evaluations, and using battle rhythm events and evaluations to reinforce accountability. The success of these efforts must be girded by a shared understanding of processes and standards. To that end we

are publishing a Legion Grey Book to serve as a reference and a guide of standards and expectations. While the Grey Book serves as the bedrock upon which we are building the Legion's fundamentals, it is also provides the basis for our Legionaries to steward the Army profession as they grow into Army and cyber professionals. We are also creating both unclassified and TS repositories for business rules, SOPs, orders, and policies. Moreover, we are more aggressively using battle rhythm events and annual training guidance to improve our planning, execution, and evaluation of our training and operations.

**Goal 2:** Innovate and improve our foxhole. We seek to establish continuous improvement throughout the Legion. While this requires establishing and reinforcing an innovative and creative mindset, it more importantly requires us to harness dissatisfaction with what is broken and wrong and springboard into action to fixing the broken and righting the wrongs. Seeing trash in the hallway and picking it—organizationally writ large. To do this, we are putting the mechanisms in place to elicit problems and/or innovations as well as investments (personnel, money, time) boards dedicated to evaluating/remediating problems and implementing innovations. As a first step, the S6 has established an anonymous drop box where anyone can initiate a battalion-level response.

**Goal 3:** Develop our people. Teams, detachments, companies, sections, and some cohorts are all setting their own course of leadership development. While extremely flexible, it is inconsistent, inefficient, and episodic. Legionaries deserve better. A recent Battalion-level OPT set down the knowledge, skills, and abilities (KSAs) we expect of leaders in different cohorts (e.g. team, company, section leadership as well as master, senior, and basic work role proficiencies). These



expected KSAs form the basis of LPD and STT programs within the Cyber Legion. The Battalion program will now provide the standards (and resources) to which the companies and teams are expected to maintain. Moving forward, companies and teams will combine their own existing/ongoing LPDs and STTs with training that ensures proficiency in core Legionary KSAs.

**Goal 4:** Deliver impactful results. Outcome-focused leadership minimizes opportunity costs while maximizing yield but requires sound risk-taking, assessments, honest feedback to supported commanders, and an aggressive (but not abrasive) pursuit of results. Effective teammateship recognizes that each member of the team provides value, and excellence in the value-chain is cumulative. To support these outcomes, we are renewing the Battalion's focus on recognition of merit and prudent aggressiveness while simultaneously holding substandard performance accountable. We are reinvigorating Battalion Soldier, Civilian, and Workrole of the Quarter programs to promote achievement. Lastly, we have begun a rebranding and streamer initiative to reinforce these aspects of the Legion's identity and further acknowledge our outstanding performers.

These goals are aligned with our mission, vision, and values, and they reflect our duty to the Cyber Legion and the American people. We believe that through these goals we will improve tangible outcomes for combatant commanders as well as morale and satisfaction for our Legionaries.

This is where the 782d is headed. We invite you share your ideas and feedback with us. Our intent is to make the 782d a better place to work and a more effective platform for projecting national power. ■

# Notes on the Role of the Commissioned Officer in Cyber

By 1LT Thomas J. Bordeaux, Operations Officer/LOE Lead, 782d MI BN (Cyber)



THE CYBER OFFICER CORPS has played a strong foundational role in the history of the branch. They have played an integral role in shaping policies, defining work roles, establishing standards, and driving the Cyber Mission Force (CMF) forward to success in its various mission sets. The same weight of responsibility is borne by officers today, and we are beholden to ourselves, our Soldiers, and our Nation to continue the work of stewarding the profession and promoting positive change. Commissioned officers create conditions and hold risk; it is imperative that we create good, healthy conditions and make sound risk decisions

so that we retain the broad-spectrum talent contained within the CMF as it continues to grow, and we preserve our ability to fight and project power as we dominate within the cyberspace domain.

From my perspective as a junior officer in the 782d Military Intelligence Battalion (Cyber), a current challenge for our senior officers is defining—or, perhaps, redefining—what it means to be a Combat Mission Team operating below the level of armed conflict and atop the shifting sands of policy changes and dynamic geopolitical relations. As that definition becomes clear, our task as junior officers at the lowest echelon are to provide purpose, direction, and motivation within our

Teams, but also to perspective and scope that redefines success for a CMT beyond just effects as the sole, goal of operations. Our input may even be required for bottom-up refinement of such a revised CMT construct. My experience in Cyber is short and operationally limited to OCO under JFHQ-C (AF), but I believe the Officer Corps will play a critical role in the continued success of the CMF and our leadership must be sound as our military's capabilities within the cyberspace domain increasingly defines and shapes our ability to succeed in our mission to fight and win our nation's wars across all domains. ■







# Shaping Future Leadership in the Cyber Mission Force Through Lessons Learned

By 1LT Michael D. Mercier, LOE Lead, 782d MI BN (Cyber)

**A**N ASPIRING PILOT AT THE U.S. AIR FORCE ACADEMY to an enlisted communicator with the 75th Ranger Regiment, my military experience has been anything but typical. Though despite the varied experiences of my past, serving as a Line of Effort Lead with a Combat Mission Team has proven to be a unique and at times challenging experience. Finding a balance between the various aspects of leadership has been one of several challenges I've faced as a junior cyber officer.

My previous military experience primarily exposed me to more traditional forms of leadership, generally ranging from authoritative to authoritarian. As a Line of Effort lead in the Cyber Mission Force, adhering too closely to these traditional forms of leadership is likely a recipe for disaster. Instead, a balance between collaborative and authoritative leadership is what I've found is most effective when it comes to guiding a productive team. Collaborative leadership fosters the free flow of ideas from team

members, and that is often what is required to solve the complex problems on Cyber Mission Teams. A collaborative leadership style has the additional benefit of promoting trust and a feeling of ownership amongst team members. This is critical to morale and keeping valuable talent from leaving the Cyber Mission Force.

Leading a team of highly specialized and in many cases highly experienced technical experts in both the intelligence and offensive cyber fields requires open communication and a free flow of ideas to be successful. When coming up with solutions to complex technical problems, I often find my role to be that of a facilitator. Providing high level guidance, asking clarifying questions, and connecting my team with external resources have been my main contributions to these efforts.

Balancing pushing guidance and expectations of higher leadership versus validating the concerns and ideas of team members is another challenge. As a Line of Effort Lead there are inevitably times when your team

lead's guidance and expectations will clash with the advisements of your team. These unfortunate situations are where you will realize that despite your best intentions, you can't please everyone. Recognizing whether or not to apply pressure to attempt to overcome what your team has identified as obstacles to meeting the team leads expectations is something that cyber officers must learn to balance. Too much pressure can cause a variety of issues ranging from burn out to team member's feeling like their concerns are invalid. Too little pressure and your team may never realize their true potential.

These balancing acts are something that are one of the challenges of leadership, but they are part of what makes it rewarding. As the Cyber Force grows and matures, Cyber Officers will gather lessons learned on what works and what doesn't with regards to leadership within the Cyber Mission Force. Eventually it will become clearer what kind of leadership qualities are expected of the officers of the Cyber Mission Force. ■

# Cyber Officers: Students for Life

By 1LT Jack Summers, D Company, 782d MI Battalion (Cyber)



AS THE COMPLEXITY OF OUR WORLD INCREASES, so does the complexity of warfare. As such it is imperative that military leaders act as students for life. This concept is not new, and it holds true for all branches of the military, but commissioned officers within the Cyber have to educate themselves differently than Officers of the past. Officers must study technical material such as public Cyber certifications, or they must seek higher education covering computing topics throughout their careers. Not only do Officers need to grow from an academic standpoint, but they can also benefit from a wealth of knowledge from their Soldiers, Noncommissioned Officers, and Warrant Officers. An Officer who thinks they are the smartest person in the room is bound to be humbled sooner than later. This article will first explore some of the challenges that our Army faces, and then discuss the benefits of studying a breadth of knowledge as traditional Officers have in the past. To finish off, the paper will argue that Cyber Officers should select a computing topic and study it in depth.

General Paul Nakasone stated that “superiority in cyberspace is temporary; we may achieve it for a period of time, but it’s ephemeral. That’s why we must operate continuously to seize and maintain the initiative in the face of persistent threats.” With the incorporation of the Cyber domain, warfare has become more technical and complex. Even during “peace” time, we are constantly competing with our adversaries. Instead of balancing a bipolar world order like during the cold war period, we are currently in a code war. Just as Officers read in the past, the modern Officer must self-study to maintain the initiative. Often when people think of a soldier-scholar, they think of Lt. Col. Hal Moore played by Mel Gibson in the film “We Were Soldiers,” hunched over his history books in the dead of night studying his enemy. Lt. Col. Hal Moore is a great example for Officers to emulate. After attending West Point, he went to grad school at Harvard. Lifelong learning is critical because “by reading you learn through other’s experiences, generally, a better way to do business, especially in our line of work where the consequences of incompetence are so final for young men”

(General Mattis). However, the modern Officer cannot only read on psychology, history, and tactics as the generations before. The contemporary warfighter will also need to understand technical concepts such as a basic understanding of networking, programming, and cybersecurity, allowing Officers to understand the information environment better and be more prepared for the challenges our Country faces. Perhaps the Army aviation community is a good example to follow, for Officers must learn to fly before they lead their organizations. Cyber Officer must also know the intricacies of their domain. Everyone’s next step is different, what matters most is that you take it. Have an undergraduate degree? Pursue a master’s in a computing topic that interests you. Maybe earning a PhD can help you be a force multiplier for your unit. More college isn’t for you? Study to obtain a cyber-certificate or study for a specialized DoD work role. Being a student for life is critical to lead effectively. ■





# Hawaiian Horizons: Junior Officers Lead New Wave of Capability Development

by 1LT Reed Burton, Detachment Hawaii, 782d MI BN (Cyber)

**W**HEN ESTABLISHING a new organization, junior officers must be prepared to take matters into their own hands. With limited resources and minimal oversight, a team of remote developers has successfully launched the newest Cyber Solutions Development (CSD) Detachment on the island of Oahu, led at the time by the highest-ranking individual, an O1 graduate of BOLC. Now comprising of only a handful of developers, this organization challenges its members to be flexible and adapt to the ever-changing cyber landscape. Leveraging the unique background of the Cyber Officer Corps, this article focuses on how leaders may assume greater responsibilities than initially expected and how diverse backgrounds can foster creative solutions in a resource-limited environment.

The history of the Hawaiian Islands is steeped with stories of change and chaos. Violent volcanic activity gave way to a new emerging archipelago deep within the Pacific Ocean – hundreds of miles from any other land mass. These remote isles were brought into the world with a cacophony of explosions and hurdling rock and lava.

However, there had been no creatures to populate its beautiful lands and waters yet. Over time, the islands would be found by many fish and other fauna. Some of the earliest reef fish are believed to have drifted over the open ocean as mere larvae all the way from the tropic waters of Asia-Pacific. This journey seeded the island with these creatures and only those able to survive the long trek were granted an opportunity to thrive in the rich islands of Hawaii. These islands acted as a proving ground, giving no respite to its inhabitants ensuring that through every change that only the hardy could survive.

This concept of change and adaptation exists on the islands today in the age of modern machines and computing. The 782d Military Intelligence Battalion, Detachment Hawaii sits on the island of Oahu. Holding down the western front, it operates alone in solace. Even with the miracle of modern technology, the distance can be felt. Time zone changes and latency provide several hurdles that over the course of a three-year tour can add up to a frustratingly difficult work life. Fortunately, a constant flow of TDY visitors from the home station helps

to build strong relationships with the Detachment's fair-weather colleagues.

Even more secluded than the Detachment, a small team of developers have successfully launched the newest Cyber Solutions Development (CSD) Detachment on the island of Oahu. Not dissimilar to the drifting larvae of Asian reef fish, the Army had sent a Second Lieutenant to island with little guidance and an overall unclear path forward. As a graduating member of the pilot 17D BOLC, 2LT Burton came to the realization that there were no clear assignments available for himself and his wife, an Apache helicopter pilot. The solution was to send both to Oahu with the vague goal of starting up a new CSD—one consisting of a single Basic qualified tool developer.

Upon arriving, Burton was met with a strange change of scenery. Instead of the modern utopian landscape of Augusta and Grovetown he found himself in the midst of rugged tropical beaches and free roaming chickens. These chickens, channeling their prehistoric origin as fierce reptiles, have taken over as one of the largest land animals on the island. Adapting to the times, instead of devouring



When 1LT Burton is not participating in analogue photography, vintage electro-mechanical piano repair, or looking at fish, he is conducting programming on the beach. Photo taken by CPT Zablocky



A Hawaiian Green Sea Turtle photographed by 1LT(P) Burton



CPT Zablocky displays both his passion for surfing and programming. On days with decent surf you may see him accomplishing both simultaneously. Photo taken by 1LT(P) Burton

the flesh of their fallen prey, go for an easier mark—LT Burton's food truck corndogs. Undeterred, this young LT went on with the process of creating an organization from scratch. Despite years of preparation to become an officer, a herculean task like this had never been advertised. When applying to be a 17D, there was very little expectation that a junior officer would be attempting to attach themselves to a unit like Detachment Hawaii—a unit that not-only was not expecting to receive a developer but also had no real vision of how one would be employed in isolation.

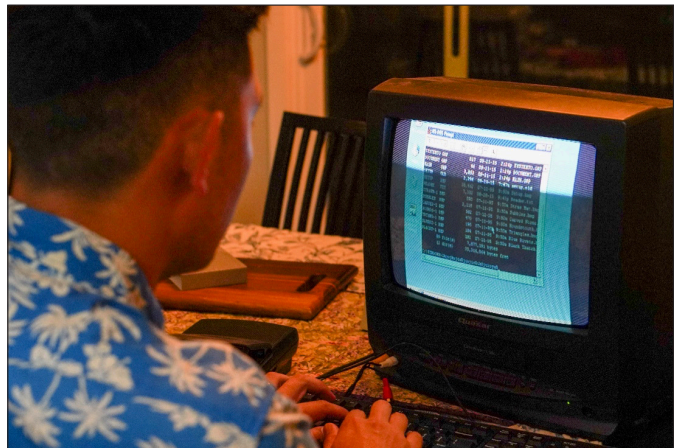
In the end, however, adaptation and survival took place. In order to adapt to their new environment, Burton had found strength in the Hawaiian spirit of aloha. A concept of inner harmony and peace through community and spirit. He had learned to lean on those around him for support and build up relationships with mentors remote and local. Using a newfound calmness and stress-free mentality, the tasks became achievable, and areas of developer involvement were identified allowing for actual impact to be made by a single developer. As time passed, the role of developers on island became clear. Assisted by personnel from partner branches and from very talented non-commissioned officers there was now the foundation of a real and meaningful organization. Popping up from nothing like the islands themselves.

As tools were developed and word made its way throughout the island, CSD-HI grew. An aspiring developer,

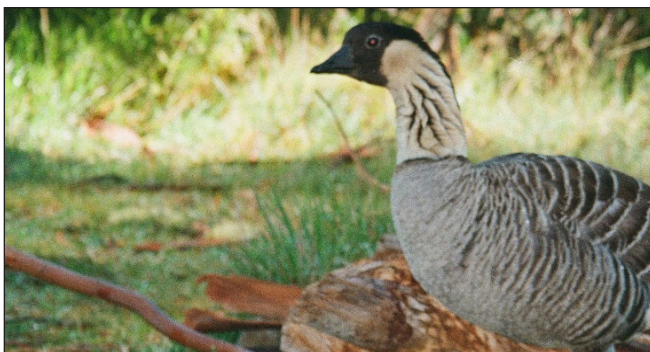
CPT Zablocky was made aware of the plight of the organization. He was no stranger to adaptation— his background of being a platoon leader in the Infantry and his transition to Cyber taught him all he needed to know about adapting and surviving. Upon completion of his developer training, he was able to join CSD-HI and add new perspective to the organization. As a leader with broad Army experience, he was able to enable the CSD to take on larger and more challenging projects. The rapid change displayed that there was indeed room for growth and that the ceiling was still unknown for this fledgling organization. Despite many believing that this assignment would be a one-off without meaningful work, there was now proof of triumph. Triumph similar to that of the Hawaiian Nēnē—a long removed relative of the Canadian Goose who has made a grand recovery from the jaws of extinction. The Nēnē met the challenges of the island and lives amongst the tallest mountain in the world. Now, both CSD-HI and the Nēnē look to a more promising future.

Through mentorship and guidance, CSD-HI

plans to continue expanding—Do you think you can take on the challenge of joining the newest team in the CSD? Are you a self-starter who can operate with minimal supervision? Do you not have Alektorophobia? Can you surf? If so, ask your branch manager for an assignment to this unique organization.



1LT(P) Burton participating in the annual President's Cup using modern technology. Photo taken by 1LT(P) Krug (the Apache pilot with a much cooler job).



A majestic Hawaiian Nēnē at Haleakalā Nation Park on Maui taken by 1LT(P) Burton on 35mm film. Despite their friendly appearance they can be found harassing tourists and weary hikers who venture a step too close.



Chickens plotting to steal corn dogs. Photo taken by 1LT(P) Burton ■





# A balance in technical and professional Officer Development

By CPT Laura C. Adams, Detachment Texas, 782d MI BN (Cyber)

**D**URING ITS INITIAL BUILD IN 2014, the Army's Cyber Branch recruited initial-entry officers with knowledge in foundational coding expertise, emerging technology, and STEM fundamentals. This recruitment tactic emphasized technical expertise over professional leadership development. As cyber capabilities became more predominant within strategies for national security, the Cyber Corps needed to address the imbalance between technical and professional leadership. The Cyber Corps addressed the issue by shifting focus to developing cyber professionals who promote innovation within the technical realm while maintaining mission command and developing cohesive operational planning within a multi-domain environment.

Leadership development, within the cyber branch's initial build, provided technical knowledge within the Basic Officers Leadership Course (BOLC) and foundational professional knowledge within the Captains Career Course (CCC). Knowledge development continued with an operational focus through on-the-job training and mentorship from other Officers, Warrant Officers (WOs), Non-commissioned Officers (NCOs), and Department of Defense (DOD) Civilians. Then, the individual must address their education and training gaps through self-development. From these conditions, United States Cyber Command (USCYBERCOM) realized that building an elite cyber force required a formalized development framework to meet operational requirements. USCYBERCOM J7 created and enforced pipeline training for the cyber force. This pipeline forces Cyber officers to include training considerations and limitations within their operational planning when meeting mission needs. However, Army

Cyber Officers realized that addressing the imbalance between technical and professional knowledge within all three developmental domains would better prepare Soldiers to meet USCYBERCOM's operational requirements. These domains are depicted in the Army Leader Development Model in DA PAM 350-58. [Figure below - developmental domains - da pam 350-58]

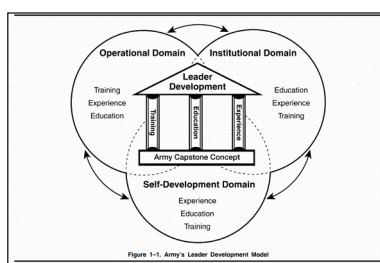


Figure 1. Army's Leader Development Model

National security strategies involving cyber capabilities set precedence for Cyber Officers to understand emerging technologies and manage multi-domain mission requirements. Striking the balance between technological and operational knowledge should begin with Professional Military Education (PME) courses. Adjustments for future PME courses should include feedback from the operational force, where the PME course framework integrates Army and Cyber generational knowledge. USCYBERCOM's next-generation directive for the Cyber Mission Force (CMF) provided a primary incentive for operational feedback. Input from the cyber force in 2018 justified updating BOLC and CCC instructions to apply Army mission command principles, orders production fundamentals, and decision-making processes to the information environment. From these updated courses, junior Army Officers retain the ability to understand the technical skills required for the cyber branch but improve proficiency

in operational planning. These courses started incorporating private industries' expertise with emerging technologies. Additionally, capturing lessons learned in managing joint operation missions is crucial for understanding the multi-domain environment. This course adjustment set the tone for Officers to develop effective leadership skills despite the complexity of mission, environment, and team management. Shared generational knowledge within the cyber community shifts one's development from the institutional to the operational domain. This shared knowledge comes from within the Officer Corps, WO Corps, NCO Corps, and the Civilian Corps. Continued growth and development are not always linear, but they are vital in cultivating a learning culture through shared generational knowledge within the cyber community. In addition to adjusting institutional development requirements, the Army Cyber Branch uses a modern talent development method called the "s" learning curve when mentoring and developing Soldiers.

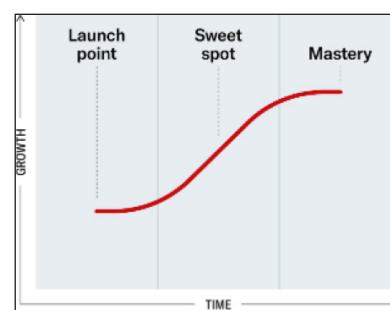


Figure 2. Army's Leader Development Model

Within the operational development domain, progress through on-the-job training and development can be outlined through the "s" learning curve. As described by Whitney Johnson in the Harvard Business Review, leaders use the



“s” learning curve for talent development to observe and guide team member’s trajectory in competence and role expertise. The bottom of the learning curve begins with the “launch point,” which signifies gradual initial learning and growth in a new role. The “sweet spot” is where the effort of learning is proportional to overcoming setbacks through rapidly learning and acquiring new skills within the role. The last phase of the curve signifies where one reaches the peak of their role expertise, and there is little left to learn within the role (Johnson, FEB 2022). This concept also applies to junior Officers when they arrive at a new position. As one stretches and moves through on-the-job training, foundational work-role skills form after working and leading through complexity and embracing humility.

Additionally, initial-entry roles for junior Officers provide the most exposure for understanding the organization one serves. In this role, significant developmental growth in learning to advocate for team members and manage mission requirements does not occur within one’s comfort zone. The nature of the mission and the leadership role requirements will overwhelm anyone. But when paired with imposed pressure, these factors are not a reason to make rash decisions. The perspective of the “s” curve highlights that input from the cyber community drives changes to the operational developmental domain. Therefore, receiving feedback from teammates within the WO Corps, NCO Corps, and Civilian Corps is imperative to help Officers maintain and advocate for better expectations, guidance, and direction. Adversity exercises skills from training or operational experiences and highlights the educational gaps in the institutional and operational domains. The individual must address these gaps through self-development.

Officers must learn “soft” skills through self-development to transition from requesting “experienced and trained” individuals to advocating for opportunities to develop team members into trained and experienced professionals. Sometimes, as leaders, we must create those opportunities

and learn to grow where the current situation within the organization plants us. Through self-development, junior officers must improve in anticipating their higher command’s priorities. This proactive mindset creates the predictability the team desires when operational requirements drive changes within higher leadership’s direction.

After the investments in developing junior Officers, it is imperative for Officers to give back to the cyber community. From reflection on lessons learned from all three development domains, one should pass on the knowledge through operational mentorship or provide feedback for improvement within the professional development framework. The lessons will look different for everyone, but the most common themes include learning to use one’s professional knowledge to care for people and one’s technical knowledge to manage the mission and workplace relationships.

Future operations will require the Officer Corps to become more proactive in learning and advocating for training about emerging technology. Many training considerations reflect reactive observations of more recent cyber news events. Operational and training opportunities with more adaptive justifications will build and strengthen the Cyber Corps to face upcoming challenges. This action represents fulfilling requirements for developing leaders, as depicted in FM 6-22, Chapter 2. [Figure below – developing leaders fundamentals] As multiple expert perspectives enter a team, leaders must integrate these perspectives to create a complete operational picture for the team

to work toward. This action is necessary to stay ahead as cyber adversarial tactics become more sophisticated.

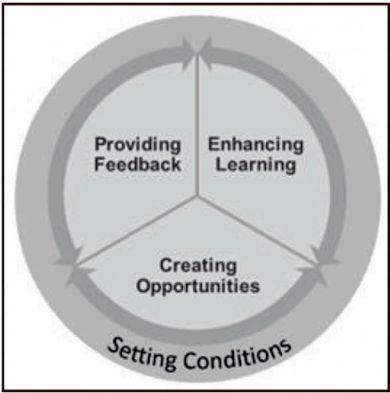


Figure 3. Fundamentals of developing leaders.

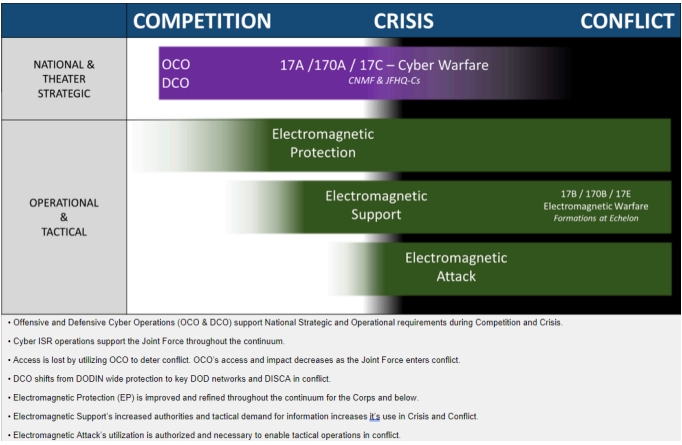
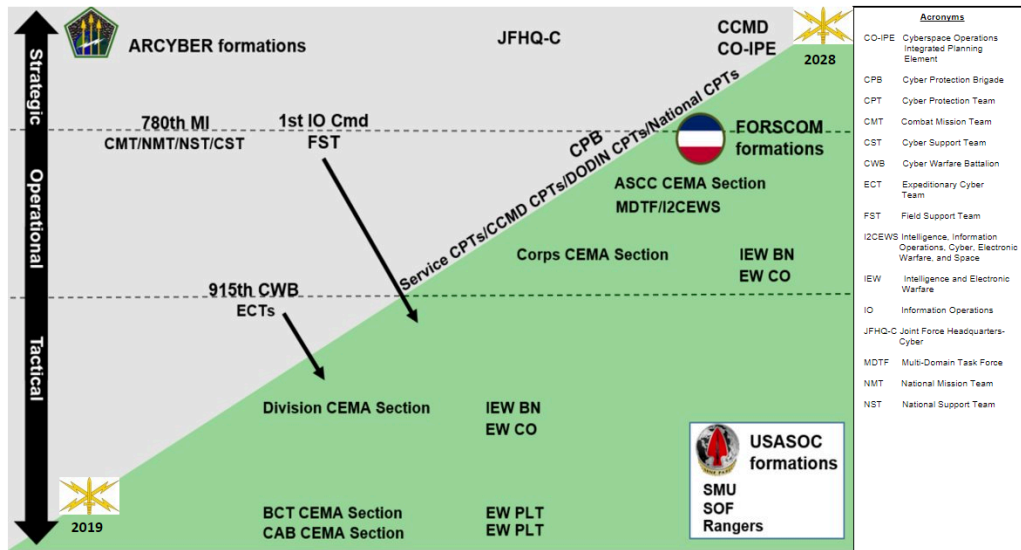


Figure 3. Fundamentals of developing leaders.

As learned in recent military history, new tools and technologies within the battlespace have caused the re-evaluation of the conflict continuum and how the Cyber Corps will contribute to future engagements. [Figure above – conflict Continuum]. The operational environment requires the cyber corps to evolve from focusing on cyber campaign plans to being more synced with multi-domain operations. This requirement adjusted the future projection of the 17-series Officers ratio within ARCYBER and FORSCOM formations. [Figure below - Changes in Officer Assignments].

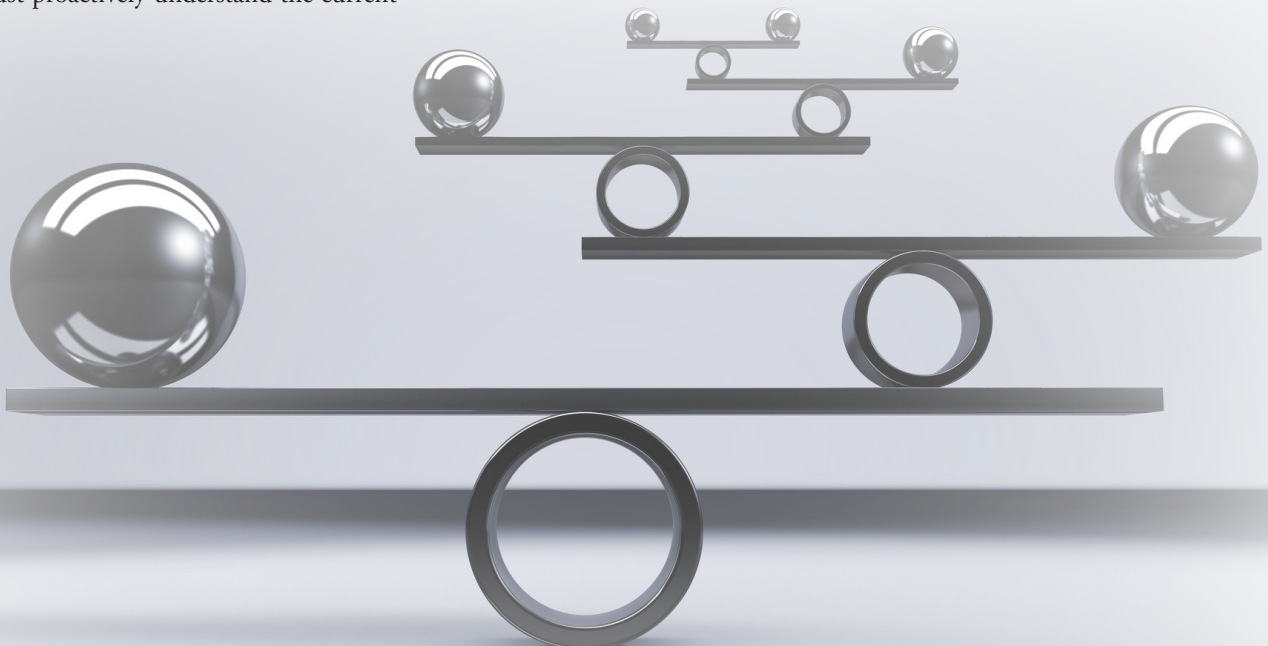


Officer development has evolved since 2014 in addressing the imbalance within technical and professional knowledge. National security strategies drive the changes made to the institutional and operational domain. The new requirements from USCYBERCOM's initiative for next-generation CMF drive the Army Cyber Branch to transfer generational knowledge from the cyber community to PME courses and refine on-the-job training within the operational environment. To meet the enduring need to match security strategies, Officers must proactively understand the current

situation and anticipate operational and professional requirements to face battlespace challenges. Understanding how one's leadership analyzes the situation and the multi-domain environment will enable one to advocate for training and operational opportunities for one's team. As a community, we can better impose costs by building and strengthening a more balanced cyber community by driving proactive actions in PME courses, operational training, and mentorship within institutional, operational, and self-development domains.

#### References:

- <sup>1</sup>DA PAM 350-58, 08 MAR 2013, Army Leader Development Program, [https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/pdf/web/p350\\_58.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/p350_58.pdf)
- <sup>2</sup>FM 6-22, 01 NOV 2022, Developing leaders, [https://armypubs.army.mil/epubs/DR\\_pubs/DR\\_a/ARN36735-FM\\_6-22-000-WEB-1.pdf](https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36735-FM_6-22-000-WEB-1.pdf)
- <sup>3</sup>Johnson, W. (FEB 2022) "Manage Your Organization as a Portfolio of Learning Curves". Harvard Business Review. <https://hbr.org/2022/01/manage-your-organization-as-a-portfolio-of-learning-curves>



# Task Force Future

By MAJ Ben Liles and MAJ Michael Krogh, Task Force - Praetorian



## Where We've Been

**T**HE CYBER MISSION FORCE was built upon the speculation that our enemy would fight like we do in the cyber domain. Our task organization followed the dogma of self-contained units capable of a wide variety of functions with an adaptive flexibility for any environment. The 780th Military Intelligence Brigade (Cyber) was at the forefront of defining those units and their composition, finely tuning and creating efficiencies with each iteration. We employed our forces to United States Cyber Command, the Cyber National Mission Force, and the Joint Force Headquarters, each with their own nuances, requirements, and objectives. As we accomplished each mission, leadership throughout the formation learned to understand the cyber environment and aligned their elements to meet increasingly complex operations.

These elements are fundamentally separated into two components: operations and operations support. Force structure design purposefully kept these components small to facilitate rapid adaptations and reduce the amount of overhead necessary for collaboration. Cyber operators relied upon their assigned analysts, linguists, and capability developers for every mission, working closely with them to gain access to and deliver effects against mission objectives. However, over time it became clear that creating isolated teams introduced an artificial limitation: teams only had access to resources directly assigned to them.

## Where We're Going

The organization inevitably gravitated towards instituting changes to achieve optimization and utilization. Elements within the CMF refused to be at the mercy of a decade's old organizational structure. CNMF was one of the first to realize such changes and implemented a sub-unified command to enhance their ability to impose costs upon our adversaries. In 2023, Colonel Benjamin Sangster, the commander of the 780th MI BDE, capitalized on the opportunity to begin consolidating his support elements. This concept became reality through the formation of Task Force Praetorian (TF-P), an ad-hoc organizational built organically from personnel within the brigade, complete with staff and the necessary resources to satisfy administrative requirements.

Major Marissa Cina, the first commander of TF-P, led the unit's growth, structuring, and alignment. One primary benefit of the change was the formalization of the Cyber Solution Development (CSD) Detachment's support model. The CSD contains every developer aligned against National and Combat Support Teams. Through the consolidation, CSD reaps the benefits of specialization, training, and support. Instead of teams being limited to whatever developers are assigned to them, the entire CMF can request support from centralized knowledge, technical expertise, and cyber support. This unified, enterprise model requires a unique skillset to manage.

The unique nature of the CSD was one

of the key drivers to consolidation and change. While developers are consolidated under a single organization, there are several development cells positioned geographically adjacent to their supported commands. The management of these sites – located in Georgia, Texas, Maryland, and Hawaii – was perfectly suited to the design and structure of TF-P. With plans to extend CSD to additional locations, the capacity for 780th to provide world-class capability development support improves as well as our ability to manage resources and preserve combat power.

The benefits of consolidation do not necessarily need to stop with our developers, as this can translate towards other operational support elements that could help enable the operational force. Leaders should have the ability to pull form a bench of expert linguists, analysts, and other enablers to give them the expertise and responsiveness needed when addressing an array of problems.

The Task Force is the result of over a decade of cyber operations. Our leaders continue to recognize the differences of the cyber domain and leverage its near instant operational speed. Missions move at a velocity that demands a broad spectrum of dynamic support. No one team has the answer and not every operator can solve all the problems, but as we look to the future, and position our enablers, we posture ourselves to triumph over any obstacle. ■





# Cyber Leader's Conference at West Point

By MAJ Mark Klink, Task Force – Praetorian, Operational Support Element, 780th MI BDE (Cyber)

**A**FTER A SHORT DRIVE UP TO WEST POINT, I checked into the historic Thayer Hotel on the banks of the Hudson River and picked up my conference badge and welcome packet from a table in the lobby. Inside the packet, I found things like a schedule, a map of the installation, and a badge. But interestingly enough, the badge appeared to have a near-field communication (NFC) chip taped to its back which piqued my curiosity. I immediately went back to the hotel room, dumped the contents of the badge, and stumbled upon a rabbit hole that would serve as a continuous thread throughout the conference.

I was attending the 2024 Cyber Leader's Conference, hosted by the West Point class of 1970 and the Army Cyber Institute, as just one of many active-duty

Cyber officers from across the country. The conference was a unique opportunity to bring together all of the ROTC and West Point cadets across the country that have been identified to commission into the Cyber branch in the next year. The conference also brought in Cyber NCOs, Warrant Officers, and Officers from across the Cyber Mission Force and FORSCOM to talk about challenges and opportunities when it comes to serving as a company grade officer in the Cyber branch.

Later that first evening, during a mixer in the hotel lobby, the first part of the "badge puzzle" was revealed as a tool to encourage cadets to reach out and talk to as many active-duty participants as possible. By scanning the NFC chips on the back of attendee badges, cadets could collect points (with more points being awarded for higher ranking individuals

and multiple current or former general officers in attendance). Immediately, the room began to buzz with the sounds of interaction and discussion as the cadets and their active-duty counterparts shared experiences and expectations late into the night.

The next day was kicked off with a keynote speech from both BG Brian Vile, chief of cyber and commandant of the U.S. Army Cyber and Electromagnetic Warfare School, and MG Paul Stanton, commanding general, U.S. Army Cyber Center of Excellence and Fort Eisenhower, and followed by a jam-packed day of panels, small group discussions, and networking opportunities. The theme of the conference followed a top-down approach starting with the expectations and observations of field grade officers, operational vignettes, then company





grade officer lessons learned, and finally wrapping up the day with an informal dinner. Members of the 780th Military Intelligence Brigade (Cyber) served on panels providing team lead perspectives, operational vignettes and company grade experiences. Throughout the day, a handful of individuals continued to press on with collecting badges during breakout sessions and breaks, slowly creeping up to the top of the virtual scoreboard.

Towards the end of the first day, indications of a second possible challenge started to emerge. But this time, the challenge was more focused on evaluating the technical chops of the conference attendees through basic web and binary enumeration challenges. Despite the technical nature of the career field, the cadets selected for the Cyber branch include individuals from a diverse range of backgrounds, education, and experience. The process of working through the technical challenge and exploring the hidden aspects of the badge and the conference extended additional

opportunities to network and collaborate throughout the evening.

The last day of the conference focused much more on smaller group discussions led by LTs and company grade officers, a short tour of West Point, and a quick sales pitch on the benefits of being assigned to the Army Cyber Institute. On the drive back to Maryland, the key takeaway that I had from the conference and my own experiences within the Cyber branch is common traits amongst the career field including the constant desire to think critically, seek out new and interesting technologies, and explore the boundaries between the physical and cyber domains. The “badge challenge” offered a chance to gamify the networking event in a manner that is familiar to regular attendees of hacker conferences and really succeeded in bringing together individuals with a common interest to discuss the current and future opportunities within the branch. Despite the relatively short nature of the conference, the impressions left on the cadets and the active-duty participants

will certainly persist long after the cadets have commissioned and arrived at their first assignment as a second lieutenant in 2025. ■







# AvengerCon VIII – Army Cyber’s homegrown hacker con returns

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

**A**UGUSTA, GA. – AVENGERCON VIII is an annual computer security conference hosted by the 780th Military Intelligence Brigade (Cyber) to benefit the hackers of the U.S. Cyber Command and the Department of Defense and took place at the Georgia Cyber Innovation & Training Center, February 28 and 29.

This year’s event was hosted in partnership with the Army Cyber Institute, the Army Cyber Command Technology and Innovation Center (ArCTIC), and the Cyber Infusion Innovation Center.

“AvengerCon is a computer security conference hosted by members of the 780th Military Intelligence Brigade,” said Capt. Jake Heybey, a 17C, cyberspace operations officer with the 780th MI Brigade (Cyber), and one of the lead organizers for AvengerCon VIII. “It has stuff like presentations, three tracks of speakers, we host training workshops, and we also run small village activities for attendees to participate in.”

Heybey said the event is important for three reasons.

“One is outreach. The Georgia Cyber Innovation & Training Center is a perfect example of what we’re looking for in terms of getting elements from the federal government, state governments, academia, and private industry to all be in one space and learn from and influence each another.”

The second reason is building a culture within the DoD. A big part of why we started AvengerCon was trying to get junior service members and Civilians within our units to reach out and experience the broader culture represented by larger conferences, like Black Hat or DefCon,” added Heybey. “We wanted AvengerCon to be kind of a stepping stone. If you wanted to experience or participate in that broader culture, AvengerCon can be your first and that friendly venue to start.”

And third, it’s really important to us that AvengerCon is an all-volunteer event,” said Heybey. “It’s always been a grassroots driven event and that contributes to the unit’s culture and really binds the various units together, and while we have volunteers mostly from the 780th Brigade, we also have volunteers from across Army Cyber Command, and even some from other services.”

Day one of AvengerCon was chock-full of workshops including: an introduction to module writing for the Flipper Zero; a hands-on Python programming workshop presented by Army Maj. Brent Stone, Cyber Solutions Development Detachment, U.S. Army Cyber Command (CSD-ARCYBER); an Introduction to Rootkit Development by Clark Wood, Boston Cybernetics Institute; Threat Hunting with Security Onion by Bryant Treacle, Security Onion Solutions; Introduction to Symbolic Execution by Jeremy Blackthorne, Boston Cybernetics Institute; a hands-on workshop where the participants learned GitLab CI/CD concepts and how to write effective pipelines; and Recorded Future invited attendees to participate in an exclusive Capture-the-Flag (CTF) event tailored specifically for their Department of Defense, U.S. Intelligence Community, and Federal partners.

Day two began with a talk from Col. Stephen Hamilton, Technical Director of the Army Cyber Institute, who discussed the confluence of “Leadership and Technology.”

Hamilton recalled being told by a general officer “you don’t have to be technical to be a good leader. True, that’s true. This is the viewpoint of the Army – leadership’s important; technical abilities, if you have them, kind of cool.”

However, to make his point when talking about the Army cyber branch, Hamilton used a quote from Capt.

Benjamin Allison, currently a research scientist at West Point, “An officer cannot assume risk, if they cannot understand the risk.

His argument was to strengthen your leadership and technical abilities.

Following Hamilton’s remarks, the AvengerCon VIII keynote speaker was Army Col. Matthew Veal. Veal has worked at the National Security Agency supporting the nation’s intelligence requirements with cyber in both civilian and military capacities, and talked about the origins of Army Cyber.

Veal talked about the current stark divide between the senior folks, who he calls ‘staffers’ and the junior folks, who are the ‘doers.’ He mentioned that it might be a “strange way” to start a keynote; however, the resources to fix that gap were present at AvengerCon, both the seniors and the juniors.

The senior folks were the one originally called upon by General Ray Odierno to develop and grow the cyber branch, and while they were not necessarily the ones with the right backgrounds and made mistakes, they should be recognized for getting the force where it is today.

“To really maximize the potential of our branch, we basically have to take our heads out of the sand and acknowledge the gorilla in the room,” said Veal. “The message here isn’t that we’re a terrible branch, like I said earlier, we can’t grow and move forward unless we’re honest with ourselves about the mistakes that we made.”

“The advantage right now, though, is at least the O-5, O-6 tier groups (lieutenant colonels, colonels) are a gap point. Whereas before we’re talking about folks who have never done any of this before, the current generation has been at least CMT or NMT leads (Combat Mission Team / National Mission Team); been a mission commander at least, been with you while you conducted missions,” Veal



explained they are the bridge to where the branch is going to. “My challenge for you is presence. Get away from your desks, get away from the staff (folks), and spend time with the ‘doers’. You need to understand the stress operators have, working an eight-to-12-hour op (operations), requiring absolute perfection to avoid creating an international incident, day after day after day. While also thinking I was supposed to be home at four to pick up the kids from school and if I’m in a SCIF (sensitive compartmented information facility) I can’t call them to let them know to walk home. Once you can articulate these challenges on your own without asking someone to tell me what to say then you can use your rank to push back on the really bad good idea faeries.”

Vea said the second fix is for the ‘doers’. He said a lieutenant pretty much summarized your fix when she said “We need all the old guys to retire so we can replace them.”

“She wasn’t wrong, but you’ll never have the leaders you want if you don’t stay in the Army,” explained Vea. “Basically, in about ten more years, there won’t be any excuse for any of these leadership, senior positions to be filled by someone else, never been an operator, never been an analyst, or never been a developer. Do the math, a second lieutenant operator in 2015, that first round, by 2033, (Soldier) should be an O-6. Same with the NCO side. (Soldier) should be a sergeant major, a command sergeant major.”

“My challenge again to the doers. Don’t quit the Army,” reemphasized Vea.

The third fix, Vea explained, is on the Army Reserve support side of Cyber.

“There’s already a lot of operators, analysts, (developers) in the Reserves, but none of us are aligned with missions that actually support those training certifications” said Vea, and he’s made the decision to stay in the Army Reserves to try and address that.

Following the key note address, the rest of day two provided attendees with options to attend one of three presentation tracks taking place throughout the day, and a panel discussion focused on the recent innovations and mass proliferation of

AI-driven tools, including large language models (LLMs) such as OpenAI’s ChatGPT, and other generative AI systems capable of creating or modifying text, audio, image, and video content.

The panel – Kevin Dwyer, VP of Engineering at Black Cape; Maj. Ian Garrett, U.S. Army Reserve and CEO/co-founder of Phalanx; and Dr. Ravi Starzl, Adjunct Professor at Carnegie Mellon University, hosted by 1st Lt. Adrian Naaktegeboren, U.S. Army Cyber Protection Brigade – explored topics including the current state of these tools, their current and potential uses supporting cybersecurity applications and U.S. government cyberspace operations, limitations and security flaws of these systems including prompt injection, and the potential consequences of this technology for the world’s larger information environment.

Army Maj. Skyler Onken, a 17C, is an Individual Mobilization Augmentee (IMA) Soldier with the 780th Military Intelligence Brigade (Cyber). IMAs are part of the Select Reserve and are an integral part of our modern-day force. Onken was one of the original organizers of AvengerCon.

“AvengerCon started as an idea years ago (in 2015 at an overcrowded Johnny Rockets)... The brigade was sending a number of people out to Las Vegas for DefCon and Black Hat. I was really fortunate to go,” said Onken. “One day, I was sitting with Steve Rogacki, another member of the brigade, we were discussing how it would be super valuable for the entirety of the force to get exposed to this hacker culture, hacker community, and how, obviously, it wasn’t feasible to fly everyone out to Vegas – so what if we did something of our own where we used the opportunity for the public sector to come in and interact with the military, especially within cyber and bring that hacker culture to Soldiers, many of whom join the Army interested in cyber, but haven’t really been exposed to the hacker culture and that’s where we came up with the idea.”

The very first event was very small in scope, just under a hundred people, added Onken, and was named AvengerCon because A Company, 781st MI Battalion

(Cyber) was nicknamed the Avengers, and it originally included only Soldiers and Civilians from the Avengers.

“After (the first) AvengerCon, we decided that it would be more beneficial for people if it was more inclusive, so we decided to go away from having a classified environment to just a purely unclassified environment where we could bring in more people and that would encourage more participation as well as bring in those industry people that we kind of always wanted to involve,” said Onken. “So, in year two we did (the event) at McGill Training Center (Fort George G. Meade, Maryland)... we brought in a car hacking village, an IOT hacking village, we got the same people that do the lock-picking village at DefCon (The Open Organisation Of Lockpickers, or TOOOOL), the population grew, we made invitations for people outside the unit to make it as joint as possible.”

According to Onken, over the years AvengerCon has continued to evolve. Outgrowing McGill, and was, until recently, held at the MISI DreamPort facility in Columbia, Md. This year marks the first time the event has been held outside the state where the 780th MI Brigade is headquartered, and marks new partnerships and sponsors in Augusta, Ga., the home of U.S. Army Cyber Command, and where two of the brigade’s battalions – the 782d MI Battalion (Cyber), and 11th Cyber Battalion reside – as well as our sister unit, the Cyber Protection Brigade, the Cyber Center of Excellence, and U.S. Army Cyber School.

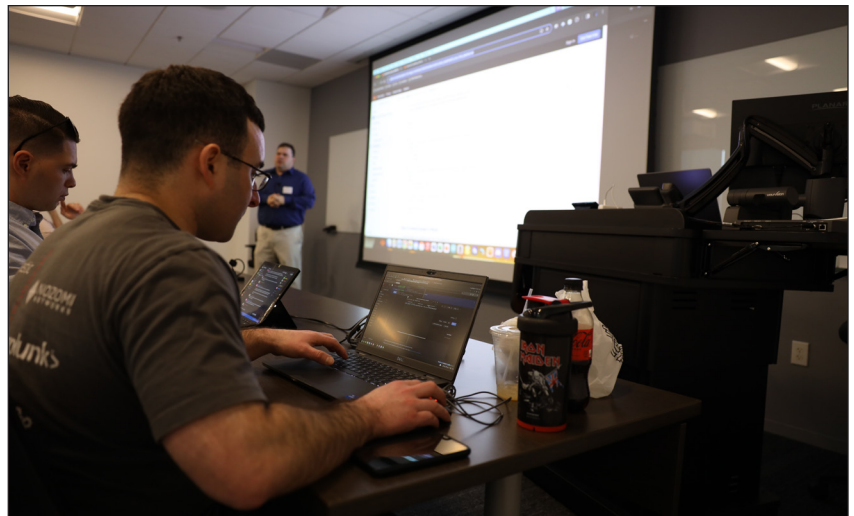
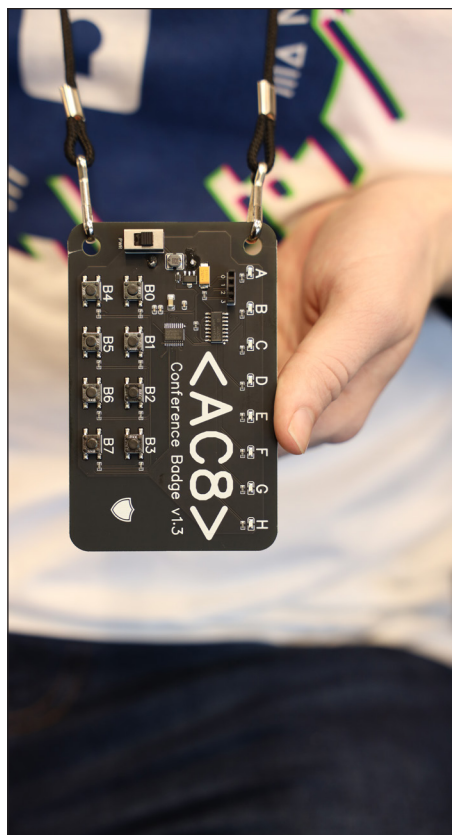
This year’s event also introduced the first ever electronic badge for AvengerCon called the “8-8-8 badge.” This conference badge doubled as a scavenger hunt to encourage participants to see all the conference has to offer. Participants either could collect codes and light up the LEDs, or hack the badge and bypass the contest altogether.

Returning AvengerCon volunteer, Army Capt. Richard Shmel, Army Cyber Institute, personally developed and made more than 300 electronic badges for this year’s event.

“Recruiting the next generation of volunteers has always been critical for

ensuring the longevity of AvengerCon,” said Army Maj. Neil Milchak, one of the lead AvengerCon VIII organizers. “With the move of AvengerCon to Georgia this year, we were especially reliant on finding a cadre of supporters in the Fort Eisenhower area. We were blessed to find a host of talented and motivated Soldiers and Civilians from the 782d MI BN, 11th Cyber BN, and others from the greater ARCYBER community to lead and help. I’m excited to see how these new contributors will drive the future of AvengerCon!”

*“Everywhere and Always...In the Fight!”*



## AvengerCon VIII – Army Cyber’s homegrown hacker con returns in Augusta for the first time

AUGUSTA, Ga. – AvengerCon VIII, Army Cyber’s homegrown hacker convention returned for its eighth iteration, and its first at the Georgia Cyber Innovation & Training Center, February 28 and 29, and, as in the past, was hosted by the 780th Military Intelligence Brigade (Cyber) with new partnerships including

the Army Cyber Institute and the Army Cyber Command Technology and Innovation Center (ArCTIC),

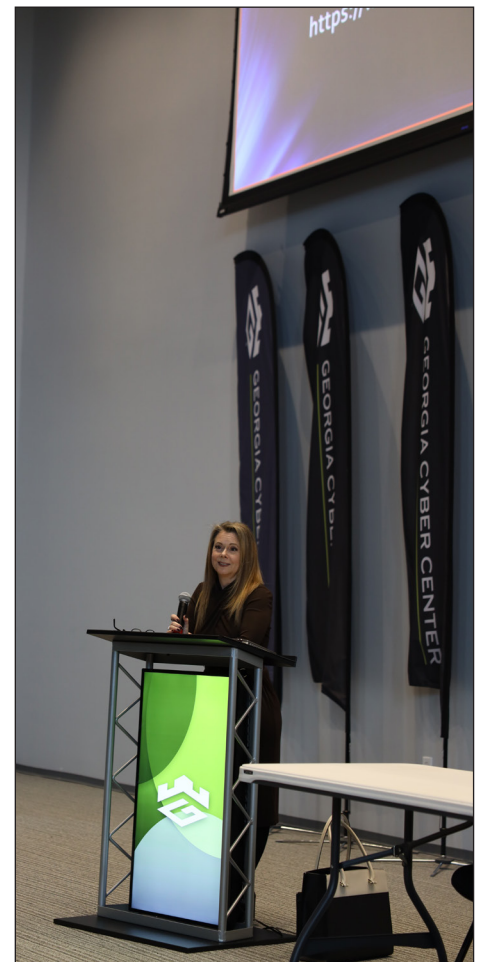
AvengerCon is a yearly free security event hosted by volunteers from the 780th Military Intelligence Brigade (Cyber) to benefit the hackers of the U.S. Cyber Command and Department of Defense. The event is targeted at personnel supporting DoD cyberspace missions, but others are welcome to attend. AvengerCon

features presentations, hacker villages, training workshops, and much more. ■









# Vanguard “When Others Cannot” Change of Responsibility



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

**F**ORT GEORGE G. MEADE, Md. – Soldiers, Family, and friends of the 781st Military Intelligence Battalion (Vanguard), 780th MI Brigade (Cyber), bid farewell to Command Sgt. Maj. Joseph P. Daniel, the battalion’s departing senior enlisted leader and ‘keeper of the colors’, and welcomed Command Sgt. Maj. Jermaine K. Ocean, in a change of responsibility ceremony hosted by Lt. Col. Donald E. Sedivy, the battalion commander, at the post theater, January 23.

Normally the timing of a battalion command team’s arrival is offset; however, they both arrived to the battalion at approximately the same time, in June 2022, and Daniel assumed responsibilities as the command sergeant major (CSM) mere minutes after Sedivy assumed command in a combined ceremony in what the two agreed was best in name of “simplicity and efficiency.”

“As I’ve come to know CSM Daniel, and reflecting on this small act of graciousness, it perfectly encapsulates the essence of CSM Daniel,” said Sedivy. “Humility, deliberateness, and care for the unit and its Soldiers and Civilians above all else.”

Daniel, who comes from an infantry and electronic warfare background, previously served as the senior enlisted electronic warfare (EW) manager with the Human Resources Command Cyber Branch and served as the Cyber Electromagnetic Activities sergeant major while assigned to U.S. Army Europe and Africa in Wiesbaden, Germany.

Among his many accomplishments in the past 20 months, Sedivy highlighted that Daniel was instrumental in the development and execution of the Vanguard Academy, a two-day training program for junior NCOs to arm them with the tools and mentorship to be effective small unit leaders; and assisting in the transition of the battalion to the

operational control the Cyber Mission Force.

Daniel’s next assignment is not far; he will assume the duties as the 780th MI Brigade’s senior enlisted leader in a couple months.

In addition to thanking the Vanguard Soldiers and Civilians, past and present, Daniel stated he was humbled by their “professionalism and dedication” that not only surpassed his expectations but set standards across the Cyber National Mission Force, Army Cyber Command (ARCYBER), Cyber Command, and the Army.

“They spend long hours countering our adversaries and your hard work does not go unnoticed,” said Daniel. “You are on the forefront of operations as you continue to develop our weapon systems and make significant advancements to the mission.”

CSM Ocean recently served as the senior enlisted leader (SEL) of ARCYBER G3/5/7, SEL of the Joint Force Headquarters-Cyber (ARCYBER), and the Noncommissioned Officer in Charge (NCOIC) of the 400

Cyber Protection Team.

“He’s a former drill sergeant, team NCOIC, and first sergeant who cares deeply about people and driving toward outcomes,” said Sedivy. “I look forward to you taking the Vanguard to new heights and to do things ‘When Others Cannot.’”

In his closing remarks Ocean quoted Theodore Roosevelt Jr. who once said, “people don’t care how much you know, until they know how much you care.”

“With the many different jobs, positions, and work roles within this organization, my main focus is to take care of the real priority...the people,” said Ocean. “I will not promise to always get it right. I will not promise you to always have the right answers; however, I do promise to always give you all I have to give. I do promise to always make decisions that I think best for the Soldiers and Civilians of the 781st MI Battalion, and I charge each of you to hold me accountable for those promises.”

“With that...781st...Let’s get it! ‘When Others Cannot’ Vanguard 7 signing on.



*FORT GEORGE G. MEADE, Md.— Soldiers, Family, and friends of the 781st Military Intelligence Battalion (Vanguard), 780th MI Brigade (Cyber), bid farewell to Command Sgt. Maj. Joseph P. Daniel, the battalion’s departing senior enlisted leader and ‘keeper of the colors’, and welcomed Command Sgt. Maj. K. Jermaine Ocean, in a change of responsibility ceremony hosted by Lt. Col. Donald E. Sedivy, the battalion commander, at the post theater, January 23. ■*







# Praetorians honor one departing senior enlisted leader and welcome another

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



**F**ORT EISENHOWER, GA. – Colonel Benjamin Sangster, commander, 780th Military Intelligence Brigade (Cyber), hosted a change of responsibility ceremony whereby Command Sergeant Major Jesse Potter relinquished his responsibility of the Praetorians and ‘keeper of the colors’ to Command Sergeant Major Joseph Daniel at the Juniper Room, Eisenhower Conference and Catering Center, March 8.

To farewell Command Sgt. Maj. Potter and welcome Command Sgt. Maj. Daniel were their fellow Soldiers, Civilians, Family and friends, representing the brigade and its subordinate battalions – the 781st MI Battalion (Vanguard), 782d MI Battalion (Cyber Legion), 11th Cyber Battalion (Leviathans), Task Force – Praetorian (the brigade’s Operational Support Element), and the 126th Cyber Protection Battalion, Task Force Echo VIII, Army National Guard – as well as representatives from U.S. Army Cyber Command (ARCYBER), the Cyber Mission Force, and Fort Eisenhower.

Potter has been around since, and directly involved in, the formation of the Cyber Corps; has served as the brigade’s S-3 (operations) sergeant major, the command sergeant major for the 781st MI Battalion (Cyber), and as the senior enlisted leader for the 780th MI Brigade (Cyber) and the Cyber Protection Brigade – the Army’s only two active-duty cyber brigades – and will next serve as the ARCYBER G-3 (operations) sergeant major.

Sangster talked about the first time he met Command Sgt. Maj. Potter and how his heart raced with excitement.

“When you come across a brigade sergeant major or higher in cyber... very, very, very unique. That’s the rarity of it,” said Sangster. “He’s been the brigade S3 sergeant major, he’s been a battalion sergeant major, he’s been at the school house, he’s been a brigade sergeant major, twice... he’s done all these things,

he knows everything, he’s experienced everything, and that’s how I felt in that moment.

“I can tell you from my experience over the 17-18 months that Jesse’s been with us, I think this captures it – I (could) talk about professionalism, pride, people, passion... I think this captures it,” said Sangster. “His office is right next to mine, and you can’t count how many different people, from different cohorts, walk by my office and go to his, because if you have an issue in our brigade, or in the Cyber Corps, this is one of the Soldiers everybody goes to. Everybody knows that if they have an issue or they’re thinking through a problem, who is going to provide them sound advice and experience? This guy.

“And it goes for me as well. I’m telling you, that’s my Woobie right there. He was my Woobie without a doubt. Anytime I came up with one of my crazy ideas, first person I would talk to is right here. He was going to give me sound advice. I don’t think I ever went opposite of what Jesse ever recommended.”

For those who do not know what a Woobie is, read the military.com article titled “Why the Woobie is the Greatest Military Invention Ever Fielded,” or read the Amazon reviews on purchasing a Woobie.

In his remarks, Potter discussed the reason the ceremony was held at Fort Eisenhower and not at Fort George G. Meade, Maryland, where the brigade is headquartered.

“The Praetorians are geographically dispersed across the entire United States from Fort Meade, Maryland, across the ocean to Schofield Barracks, Hawaii, Joint Base San Antonio, and right here at Fort Eisenhower,” explained Potter. “Actually, two-thirds of our brigade calls CSRA (Central Savannah River Area) their home projecting power from our operational headquarters less than a mile across post.”

Although he couldn’t list all the brigade’s accomplishments – it’s classified – nor could he thank every Soldier and Civilian throughout the brigade, although he honestly would have, he did say “whether it is operational accomplishments, physical prowess or excelling at traditional Army schools and professional military education, you truly have embodied the essence of Praetorians... We are ‘Everywhere and Always...In the Fight! This We’ll Defend. Praetorian 7 logging off.”

Command Sgt. Maj. Daniel is no stranger to the brigade having previously served as the 781st MI Battalion (Cyber) senior enlisted leader.

“To the Soldiers and Civilians of the brigade,” said Daniel. “Our young history was already read, but the true strength lies in its people, and I know from the time served as a battalion command sergeant major that we are stacked with professionals, dedicated to success in the defense of our country. You are the tip of the spear of our nation’s offensive cyberspace capabilities, our mission is critical and you are the best in the world.

“I look forward to getting to know all of you more as we train hard to become masters of our craft, build disciplined leaders and teams, while having fun along the way.”





*FORT EISENHOWER, Ga. – Command Sgt. Maj. Joseph Daniel (right), the senior enlisted leader and 'keeper of the colors' for the 780th Military Intelligence Brigade (Cyber) passes the brigade colors to Sgt. Maj. Richard Harrison, the brigade S-3 (operations) sergeant major, during his change of responsibility at the Juniper Room, Eisenhower Conference and Catering Center, March 8.*





*FORT EISENHOWER, Ga. – Command Sgt. Maj. Jesse Potter (right), the outgoing senior enlisted leader and ‘keeper of the colors’ for the 780th Military Intelligence Brigade (Cyber) passes the brigade colors to Col. Ben Sangster, the brigade commander, relinquishing his responsibility, during his change of responsibility at the Juniper Room, Eisenhower Conference and Catering Center, March 8.*



*FORT EISENHOWER, Ga. . – Command Sgt. Maj. Jesse Potter relinquished his responsibility as the senior enlisted leader and “keeper of the colors” for the 780th Military Intelligence Brigade (Cyber) in a change of responsibility ceremony hosted by Col. Benjamin Sangster, the brigade commander, at the Juniper Room, Eisenhower Conference and Catering Center, March 8. ■*



Leviathan Warriors are committed  
to **READINESS!**



FORT EISENHOWER, Ga. – 11th Cyber Battalion (Leviathans) hosted Lt. Gen. Maria Barrett, commanding general of U.S. Army Cyber Command, other key leaders and stakeholders in the ARCYBER Headquarters and the Cyber Center of Excellence, during a training and technical capabilities demonstration, January 24. (U.S. Army photo by 1LT Angeline Tritschler).



**Congratulations SSG Marchant!**  
780th MI Brigade Soldier recipient of  
Major General Harold J. Greene Award



AUSTIN, Texas – SSG William Marchant III, 780th Military Intelligence Brigade, won the individual Warfighter award and was honored at the fiscal year 2022 and 2023 Major General Harold J. Greene Innovation Award ceremony in the Software Factory Atrium, February 1.

The Major General Harold J. Greene Award is an Army writing competition focused on improving Army acquisition. The competition was established in 2014 to encourage all individuals to share their ideas, insight, and experiences for improving Army acquisition.



**D Company (Dracones)  
782d MI BN (Cyber)  
Change of Responsibility**



FORT EISENHOWER, Ga. – Delta Company (Dracones), 782d Military Intelligence Battalion (Cyber Legion), hosted a change of responsibility ceremony for 1SG Michael D. Olsen, the outgoing senior enlisted leader and 'keeper of the colors', and welcomed 1SG Jermaine L. Baker, at the Fort Eisenhower Friendship Chapel, February 2. Burn it Down! (U.S. Army photos by SSG Torin Marion)



**HHC (Gladiators)  
782d MI BN (Cyber)  
Change of Responsibility**



FORT EISENHOWER, Ga – Headquarters and Headquarters Company (Gladiators), 782d Military Intelligence Battalion (Cyber Legion), hosted a change of responsibility ceremony for 1SG Michael C. Thiel, the outgoing senior enlisted leader and ‘keeper of the colors’, and welcomed 1SG Michael D. Olsen, at the Fort Eisenhower Friendship Chapel, February 2. Support the Fight! (U.S. Army photos by SSG Torin Marion)



**D Company (Daemons)  
Task Force Praetorian  
Change of Responsibility**



FORT GEORGE G. MEADE, Md. – D Company (Daemons), Task Force Praetorian, 780th Military Intelligence Brigade (Cyber) change of responsibility ceremony whereby First Sergeant (1SG) Marcel Gonzalez relinquished his authority as the company's senior enlisted leader and 'keeper of the colors' to 1SG Antraun Glover in a ceremony hosted by Captain Scott Horras, the company commander, at the McGill Training Center, February 7.



**HHC (Hastati)  
780th MI Brigade (Cyber)  
Change of Command**



FORT GEORGE G. MEADE, Md. – Headquarters and Headquarters Company (Hastati), 780th Military Intelligence Brigade (Cyber) Change of Command ceremony whereby Captain Allan Baily relinquished his command to Captain Mary Watkins in a ceremony hosted by Colonel Benjamin Sangster, the brigade commander, at the MG DeKalb Army Reserve Center, February 8.



## APEX FLEX!



FORT EISENHOWER, Ga. – Apex Company, 11th Cyber Battalion, completed the Marine Corps obstacle course, February 9. Apex Soldiers are committed to staying READY, while building esprit de corps; completing the challenge together. TRAIN HARD, FIGHT HARD, WIN EASY! LEVIATHAN STRONG! (U.S. Army photos by 1LT Angeline Tritschler)







**A Company (Cyber Archers),  
782d MI BN (Cyber)  
Change of Command**



FORT EISENHOWER, Ga. – A Company (Cyber Archers), 782nd Military Intelligence Battalion (Cyber) Change of Command whereby Captain Matthew Rinaudo relinquished his command to Captain Rachel Bostick in a ceremony hosted by Lieutenant Colonel Kirklin Kudrna, the battalion commander, at the Fort Eisenhower Golf Course, February 9. (U.S. Army photos by SSG Torin Marion)



**A Company (Cyber Archers)  
782nd MI Battalion (Cyber)  
Change of Responsibility**



FORT EISENHOWER, Ga.— A Company, 782d Military Intelligence Battalion (Cyber), Soldiers, Civilians, and Family bid a fond farewell to 1SG Byron D. Armstead Jr. and welcomed 1SG Paul W. Murphy in a Change of Responsibility ceremony at the Bicentennial Chapel, February 23. Cyber Legion, Silent Victory (U.S. Army photos by SSG Torin Marion)

"Everywhere and Always...In the Fight!"



## Kopianas Soldiers fellowship



HONOLULU, Hawaii – The 782d Military Intelligence Battalion (Cyber) Unit Ministry Team, led by Chaplain (Capt.) Kevin Calmes, hosted a training, dinner, and fellowship event in downtown Honolulu for the 782d Detachment Hawaii (Kopianas) Soldiers and their Family members, February 14.



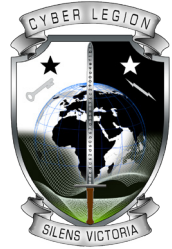
## Hastati Bowling event



FORT GEORGE G. MEADE, Md. – Soldiers and Civilians from the Headquarters and Headquarters Company (Hastati), 780th Military Intelligence Brigade enjoyed some downtime to enhance and build upon their existing camaraderie and esprit de corps at The Lanes bowling center, February 15.



## Oorah and Hooah!



FORT EISENHOWER, Ga. – Maj. Gen. Ryan P. Heritage, the current commander of U.S. Marine Corps Forces Cyberspace and U.S. Marine Corps Forces Space Command, participated in a physical training (PT) session with the Soldiers of the 782d Military Intelligence Battalion (Cyber) Combat Mission Team that supports the Marine Corps on Barton Field, February 26. The events were structured to be like the ACFT (Army Combat Fitness Test) and included circuit training at multiple different stations. Cyber Legion, Silent Victory (U.S. Army photos by SSG Torin Marion)



Oorah and Hooah!





## Hold Me Tight



AUGUSTA, Ga. – The 11th Cyber Battalion (Leviathans) Unit Ministry Team, led by Chaplain (Capt.) Ray Moore, hosted a training event for 24 Soldiers and their spouses using the Created for Connection: The “Hold Me Tight” curriculum, February 9. The training emphasized emotional connection, encouraging Soldiers to develop conversational skills to know their significant other and how to work towards stable, long-term, committed relationships. During the training, participants received instruction, enjoyed a catered dinner, and each couple also received a book, either Created for Connection (Christian perspective) or Hold Me Tight (non-religious perspective).



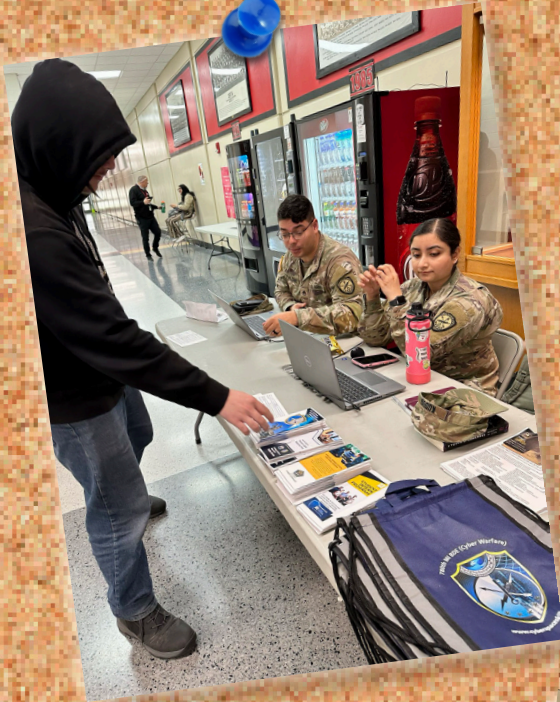
## Leviathan Strong!



FORT EISENHOWER, Ga. – B Company (Bandits), 11th Cyber Battalion (Leviathans) zeroed and qualified with their individual and crew-served weapons, including the M4 Rifle, and M249, M240B, and M2 50 Cal machineguns, flexing their technical and tactical skills to build their confidence in their kinetic arsenal. (U.S. Army photos)



## Praetorian Soldiers talk to students about Army opportunities



Loves Park, Ill. – Cyberspace operations specialists, analysts, and linguist Soldiers from the 780th Military Intelligence Brigade (Cyber) are supporting the Loves Park Recruiting Company, US Army Recruiting Command (USAREC), March 4 through 8, to talk to students about Army possibilities and opportunities. "Everywhere and Always...In the Fight!"



## Praetorian Senior Civilian Advisor Farewell



ODENTON, Md. – Army Civilians assigned to the 780th Military Intelligence Brigade (Cyber) bade a fond farewell to Greg Platt, the brigade's senior civilian and an organization 'plank holder' – symbolizing his service with the brigade since its activation on October 1, 2011. "Everywhere and Always...In the Fight!"



## Cyber Soldiers participate in the Bataan Memorial Death March 2024



WHITE SANDS MISSILE RANGE, N.M. – Soldiers from Detachment Texas (Cyber Rangers), 782nd Military Intelligence Battalion (Cyber), representing the 780th MI Brigade (Cyber), participated in the Bataan Memorial Death March 2024, Team Military Division, and finished 22nd out of 66 military (including ROTC) teams – 23rd out of 74 overall, March 16 (U.S. Army Courtesy Photos).

While in the area, the Cyber Ranger Soldiers supported the El Paso Recruiting Company, Texas, and visited two local high schools – Austin High School and Ysleta High School – to share their firsthand knowledge of what their lives are like while serving in the Army. #ArmyPossibilities #Beallyoucanbe



## Task Force Praetorian Operational Support Element Change of Command March 2024



FORT GEORGE G. MEADE, Md. – 1st Sgt. Summer Zakar, the senior enlisted leader and 'Keeper of the Colors' for Task Force Praetorian, 780th Military Intelligence Brigade (Cyber), prepares to pass the colors during a change of command ceremony whereby Maj. Ben Liles relinquished his command of Task Force Praetorian and director of the Capabilities Support Detachment to Maj. Michael Krogh, at the McGill Training Center, April 1.



FORT GEORGE G. MEADE, Md. – Maj. Ben Liles (right), the outgoing commander of Task Force Praetorian, passes the organization colors to Col. Benjamin Sangster, commander of the 780th Military Intelligence Brigade (Cyber), signifying his relinquishment of command, during a change of command ceremony at the McGill Training Center, April 1.



FORT GEORGE G. MEADE, Md. – Maj. Michael Krogh (left), the new commander of Task Force Praetorian, receives the organization colors from Col. Benjamin Sangster, commander of the 780th Military Intelligence Brigade (Cyber), signifying his acceptance of command, during a change of command ceremony at the McGill Training Center, April 1.



# Unit History

## Task Force Praetorian (Cyber)

THE 780TH MILITARY INTELLIGENCE BRIGADE (CYBER) was activated on 1 October 2011, as a Major Subordinate Command under the U.S. Army Intelligence & Security Command (INSCOM), serving under the operational control of U.S. Army Cyber Command (ARCYBER). The 780th MI BDE officially unfurled its colors for the first time during a ceremony at Fort Meade, Maryland on 01 December 2011. As the first cyber brigade in the Army, the unit was established to conduct cyber operations and sustain the growing need for a tactical computer network operations force.

In November 2022, 780th MI BDE established Task Force Praetorian (TF-P), headquartered at Fort Meade to consolidate and support the unit's key mission enablers. Subsequently, the geographically aligned-Combat Mission and Support Teams, the Capabilities Support Detachment, and the Joint Mission Operation Centers comprised the newest addition to the brigade's force structure. The establishment of TF-P ensures uninterrupted cyberspace operations and capability development to provide greater operational strength and capability depth.

In October 2022, the Empire joined 781st MI BN and changed its designation to Foxtrot Company. With the standup of TF-P, the company rapidly changed designation to HOC, Task Force Praetorian, 780th MI BDE. In April 2023 Delta Company, 781st MI BN changed its designation to Delta Company, Task Force Praetorian bringing with it the Army's world class developers spanning multiple geographic locations in Georgia, Texas, and Maryland. Following consolidation of the companies, Task Force Praetorian was officially approved by Department of the Army in July 2023, and formally recognized as the INSCOM Operational Support Element (OSE) on 1 March 2024. ■





# Task Force Praetorian Operational Support Element Change of Command



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

**F**ORT GEORGE G. MEADE, MD. – Col. Benjamin Sangster, commander of the 780th Military Intelligence Brigade (Cyber), hosted a change of command ceremony whereby Maj. Ben Liles relinquished his command of Task Force Praetorian and director of the Capabilities Support Detachment to Maj. Michael Krogh, in front of their fellow Soldiers, Family and friends at the McGill Training Center, April 1.

In November 2022, the 780th MI Brigade (Cyber) established Task Force Praetorian (TF-P), headquartered at Fort Meade to consolidate, and support the unit's key enablers. Subsequently, the geographically aligned-Combat Mission and Support Teams, and Capabilities Support Detachment (CSD), and the Joint Mission Operations Centers comprised the newest addition to the brigade's force structure. TF-P was officially approved by the Department of the Army in July 2023, and formally recognized as the U.S. Army Intelligence and Security Command Operational Support Element on March 1, 2024.

"Typically, we want our commanders

to have more than eight months in the seat. In Ben's case, Army happens," said Sangster. "In the cyber career field, there are certain job opportunities that you just don't pass up. Ben has been given a great opportunity to lead one of the Cyber National Mission Force National Cyber Protection Teams. It is one of the last pieces of the cyber career puzzle that Ben was missing. A key developmental, lieutenant colonel position that will round out Ben's operational experience, preparing him for future success as a senior field grade officer." Although only in command for eight months, Sangster mentioned the success Liles has had in maturing the organization; participating in the brigade's UIC (Unit Identification Code) consolidation – a six-character alphanumeric code that uniquely identifies each U.S. Department of Defense organization; helping shape the way ahead for Cyber Assignment Incentive Pay reform; and codifying how TF-P commands and controls the brigade CSDs that are geographically dispersed in support of combatant command and national requirements.

"To all the Soldiers and Civilians in the Task Force. All the credit in the world

goes to you at the companies, teams, sites, and staff," said Liles. "You did all the hard stuff, you executed mission, developed world class capabilities, and came up with processes and policies to help solidify TF-P as we grew and expanded our formation." Krogh, the new TF-P commander, is "no stranger" to the 780th and TF-P.

"He has been a member of the 780th for several years now, making his way through a special program known as CNODP (Computer Network Operations Development Program) – a program the Army uses to help produce capability developers," said Sangster. "He made a name for himself leading CSD-Maryland, which is now part of TF-P. And when Ben Liles was selected to lead a National CPT, I wasted no time selecting Michael as the next TF-P commander."

To close the ceremony, Krogh stated, "I've worked with many of you over the years and I'm constantly humbled by how wildly intelligent and talented you all are. Together, let's embrace the challenges ahead and make a difference worthy of our team's potential."

"Everywhere and Always...In the Fight!"



*FORT GEORGE G. MEADE, Md. . – Col. Benjamin Sangster (center), commander of the 780th Military Intelligence Brigade (Cyber), hosted a change of command ceremony whereby Maj. Ben Liles (right) relinquished his command of Task Force Praetorian and director of the Capabilities Support Detachment to Maj. Michael Krogh (left), in front of their fellow Soldiers, Family and friends at the McGill Training Center, April 1. ■*



**N**EXT QUARTER'S BYTE IS focused on the Brigade's Noncommissioned 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](mailto:steven.p.stover.civ@army.mil) NLT May 15, 2024. Final articles are due May 31.

