780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 12, Issue 4

WARRANT OFFICER IDENTITY

Quiet Professional

PRAETORIANS

780th MI BDE
"STRENGTH AND HONOR"

COL Candy Boparai
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, or mail to 310 Chamberlin Avenue, Fort George G. Meade, MD 20755, or call (301) 833-6430.

"Everywhere and Always...In the Fight!
Steve Stover
Public Affairs Officer
780th MI Brigade (Cyber)
Editor, The BYTE

On the Cover

PRAETORIAN CHANGE OF COMMAND

FORT GEORGE G. MEADE, Md. – Maj. Gen. Timothy D. Brown, commanding general, United States Army Intelligence and Security Command, hosted a change of command ceremony whereby Col. Benjamin F. Sangster relinquished his command of the 780th Military Intelligence Brigade (Cyber), Praetorians, to Col. Candy Boparai in a ceremony on McGlachlin Parade Field, June 21

An Introduction to Warrant Officer Identity

By COL Candy Boparai, Commander, 780th Military Intelligence Brigade (Cyber)

PRAETORIANS, welcome to this edition of The BYTE, where we dive deep into the often-unseen world of our Warrant Officer teammates. This and the next few issues will shine a spotlight on the remarkable personal stories of the people of the 780th MI Brigade (Cyber) – individuals whose daily work takes place in the shadows of cyberspace, countering our adversaries and safeguarding our nation's digital frontiers.

As I rejoin the Brigade after some time away, I am met by familiar faces and also many new team members. Talking to people across the Brigade, I am struck by the fact that a shared humanity binds us together, underscoring the common drive and empathy that fuel our collective mission. In a realm where the battlefield is no longer defined by physical terrain but by lines of code and digital infrastructure, I find the stories of these men and women compelling. From high-stakes operations to behind-the-scenes strategies, their contributions are vital to our national security, yet their stories often remain untold.

In the pages that follow, you'll meet some of the Warrant Officers who navigate this complex, invisible battlefield with unparalleled expertise and resilience. These are the stories of innovation, personal sacrifice, and commitment. You'll hear from veterans and newcomers alike, each offering a unique perspective on their roles and experiences. You'll also hear their take on the theme for this issue, which is a seldom explored aspect of Warrant Officers – their identity in the Warrant Officer cohort. Through their narratives, we not only gain insight into the human side of cyber warfare, where every keystroke and every decision can make a world of difference, we see a bit of life as an elite Army technician and leader from their eyes.

Join me as we walk a mile in a Warrant Officer's shoes to explore the profound impact of their work, celebrate their successes, and honor their dedication. This is not just a look at the operations of our Brigade but a tribute to the individuals who embody the spirit and strength of our modern military. 🟥

PRAETORIANS

6

Brigade Command Chief Warrant Officer – An Honored Privilege

By Chief Warrant Officer 5 James Richards, Command Chief Warrant Officer, 780th Military Intelligence Brigade (Cyber)

TONY STARK ONCE USED THE PHRASE "TERRIBLE PRIVILEGE" to describe the technology that both kept him alive and enabled him to power his armored suits to battle villains. He was talking to Bruce Banner (a.k.a. the Hulk) about how Bruce could harness his own power for good, and Bruce was skeptical as he had been largely unable to control that power. Tony maintained that despite the rather extreme downside, they were obligated to use their abilities to help others. That day would turn out to be a bad one for Tony, Bruce, and the rest of the Avengers – they used those abilities to first fight amongst each other, then fight off an attack on their flying fortress and repel an alien invasion from New York. I'm no Tony Stark (well, maybe – but without the suit), and aliens have yet to invade Fort Meade, however his description of his role, him embracing his circumstances, and the attendant obligation stuck with me as I thought about what it is to be a brigade Command Chief Warrant Officer (CCWO). The role is simultaneously rewarding and incredibly taxing, filled with opportunities to make a difference but with consequences for failure more significant than any position I have held.

Formally, the Army codified the CCWO role and a similar Senior Warrant Officer Advisor (SWOA) role in late 2023 through MILPER 23-399 (https://www.hrc.army.mil/Milper/23-399). The reality is that these roles at the brigade level and above have been around for more than 20 years, but in various forms throughout the Army. The MILPER describes a CCWO who is a steward of the Army (with an emphasis on the WO cohort), a trusted advisor to the commander and staffs, a model Soldier, and an action officer whenever needed. After about 18 months in the job, I find that to be accurate but incomplete – like trying to understand what food is like from a looking at a picture.

In practice:

I am a curator of WO careers. I continuously attempt to integrate fairly distant elements of our WOs' professional lives by trying to integrate the official career maps, requirements from the operational force, positions within the brigade, various sources of manning guidance, and other independent variables to ensure the human behind the WO dots has a viable path forward. This is not a straightforward endeavor, and often requires me to help solve problems external to a WO's career in order to align things within that career. It could be described as a systems approach, if we were trying to make a vehicle work with the controls of a motorcycle, the engine from an aircraft, and interior of a submarine. Despite these institutional system mismatches, I have found unlikely allies while championing in the background for positive change – in particular with our Cyber WO Career Manager, CW4 Terry Deener.

I am a mediator and a diplomat. My time in the Cyber Mission Forces (CMF) has exposed me to long standing inter-organizational conflicts and given me some insight about where these conflicts will reappear in the future. Like other tenured Soldiers, I also have an insider's perspective of the organizations I was privileged to work with, which enables me to propagate mutual understanding during conflicts or to help interdict conflicts that arise from misunderstanding. Too often, our community has the intellectual resources and opportunity to establish cooperative and mutually beneficial efforts between organizations, but a lack of empathy or understanding allows surmountable obstacles to stop progress.

I am part of our corporate memory, and an expert librarian for that memory. This aspect of my job requires me to help the collective enterprise recall successes, failures, lessons, and unrealized opportunities in a timely way. The DOD and Army Cyber enterprises are evolving substantially, even after more than 10 years, which requires us to be able to consider our next steps in context with previous ones, or the ones we did not take previously. The toughest part of this aspect of the job is to be able to distill the useful parts of our past out of our memory without letting the sting of failure or previous rejection preemptively screen those parts out.

I am a continuation of the legacy of CCWOs that came before me. In addition to those CCWOs, I was mentored by some truly legendary Soldiers and Army Civilians, and I try to pass a little bit of what they gave me to others whenever I can during the time I have left in the Army. The Soldier who wrote my letter of recommendation to become a Warrant Officer in 2006, was himself a brigade CCWO, and he went on to become the CCWO for the Delaware Army National Guard. Seven years later, I was mentored by another brigade CCWO, and that WO went on to be the CCWO for US Army Pacific. 780th Military Intelligence Brigade has its own lineage of brigade senior WOs, called Senior Technical Advisors (STA) before my predecessor had our manning documents changed to convert the position to CCWO. Each of these people passed down a piece of the CCWO's spirit to me, not only to follow the institutional definition that was recently codified, but to embrace the human side as well. I often wreck my schedule to spend time coaching, listening, and sometimes sharing a part of my own past in the hopes that it helps someone move forward. I received no less from CCWOs myself!

Reflecting on the experience I have been given by the Army and all the people who have invested in me, Tony Stark would be right to admonish me to use what I have to help others, just like he did to Bruce. I like to think I have taken up that challenge, but as I do not have an Arc Reactor buried in my chest, nor do I turn into a large green rage monster, I think being a CCWO is more of an honored privilege than a terrible one, and it is my honor to serve our community however I can.

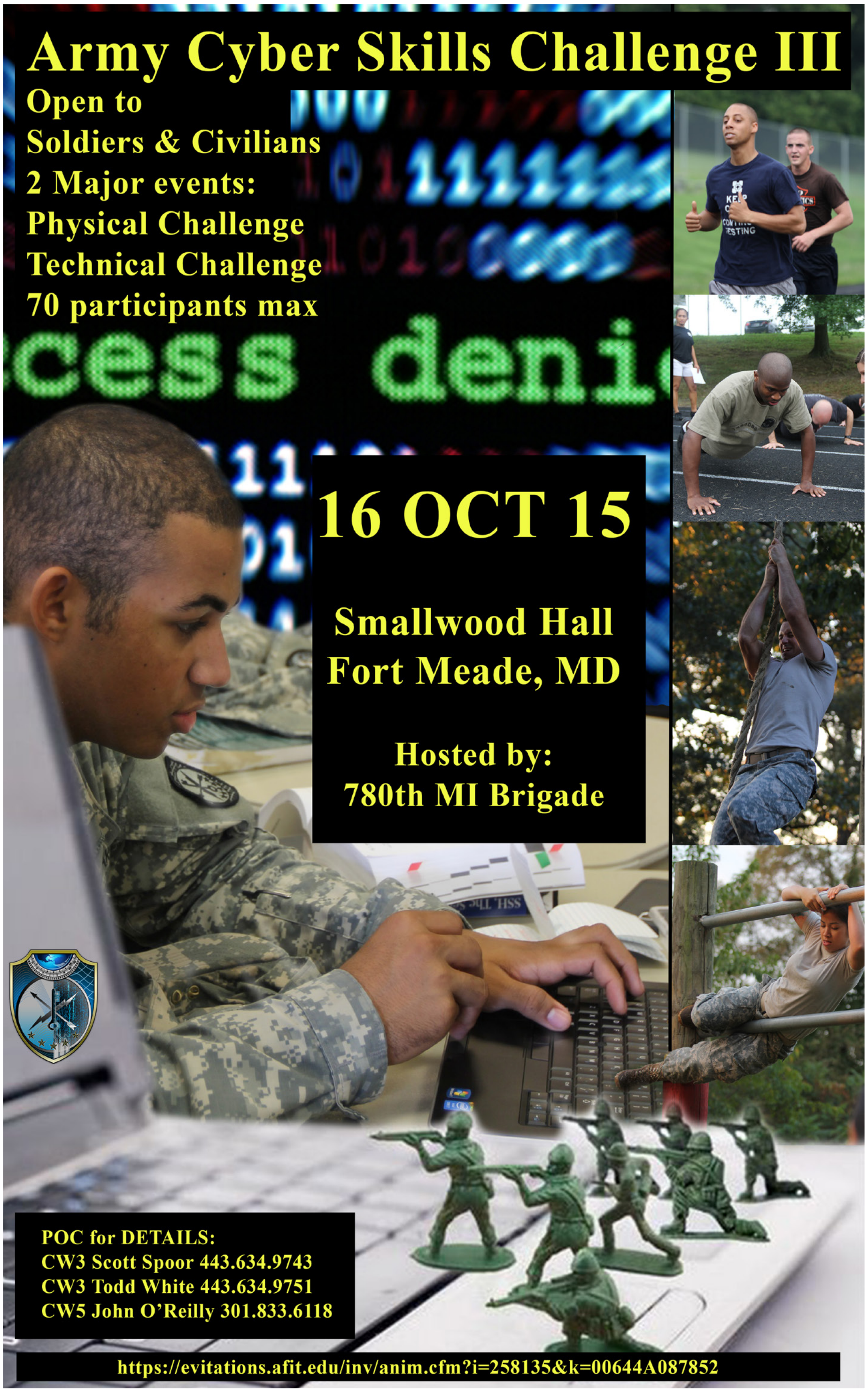
Command Chief Warrant Officer - Tracing the Brigade's WO History

By retired Chief Warrant Officer 4 Scott Spoor and Chief Warrant Officer 5 James Richards, Command Chief Warrant Officer, 780th Military Intelligence Brigade (Cyber)

ROOM 118 IN BUILDING 310R ON FORT MEADE is an unassuming room, like any other in the building. A look inside would reveal the aftermath of a technical discussion on the whiteboards, along with an accounting of 780th Military Intelligence Brigade Warrant Officer names and associated notes. A discerning eye might further catch some artifacts that keep the memory of Warrant Officers who have moved on from the brigade, and some from the Army. Still, on the surface, it is just a room. If you are in the building sometime, you can stop by to see it yourself – the door is never locked.

The room is far from ordinary, however. It is where generations of Warrant Officers have come to seek mentorship, plan coordinated efforts by the cohort, and for those who have taken the mantle of Brigade Senior Technical Advisor (STA) or Brigade Command Chief Warrant Officer (CCWO), to do the happy work of primarily helping others, be it the Brigade Commander or one of the brigade's WO cohorts. The objects in the room, passed down from the Senior WOs of the past, tell the story of the WOs in the brigade:

- Posters on the cabinet are from the Army Cyber Skills Challenge (ACSC), which was a Warrant Officer-run technical and physical competition held from 2013-2018. The ACSC III and ACSC IV posters feature the names and pictures of WOs who designed the technical challenges, ran the physical portion, and cheerfully engaged participants to build skill, morale, and interest in the early days of the Brigade.
- Doodles in one corner of the whiteboard offer a slice of life



Army Cyber Skills Challenge III

Open to
Soldiers & Civilians
2 Major events:
Physical Challenge
Technical Challenge
70 participants max

16 OCT 15

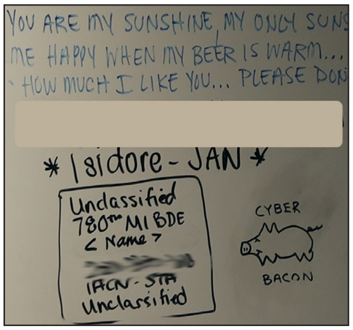
Smallwood Hall
Fort Meade, MD

Hosted by:
780th MI Brigade

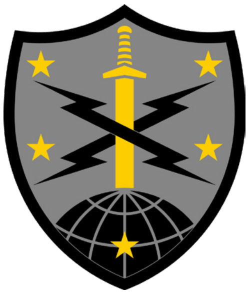
POC for DETAILS:
CW3 Scott Spoor 443.634.9743
CW3 Todd White 443.634.9751
CW5 John O'Reilly 301.833.6118

https://evitations.afit.edu/inv/anim.cfm?i=258135&k=00644A087852

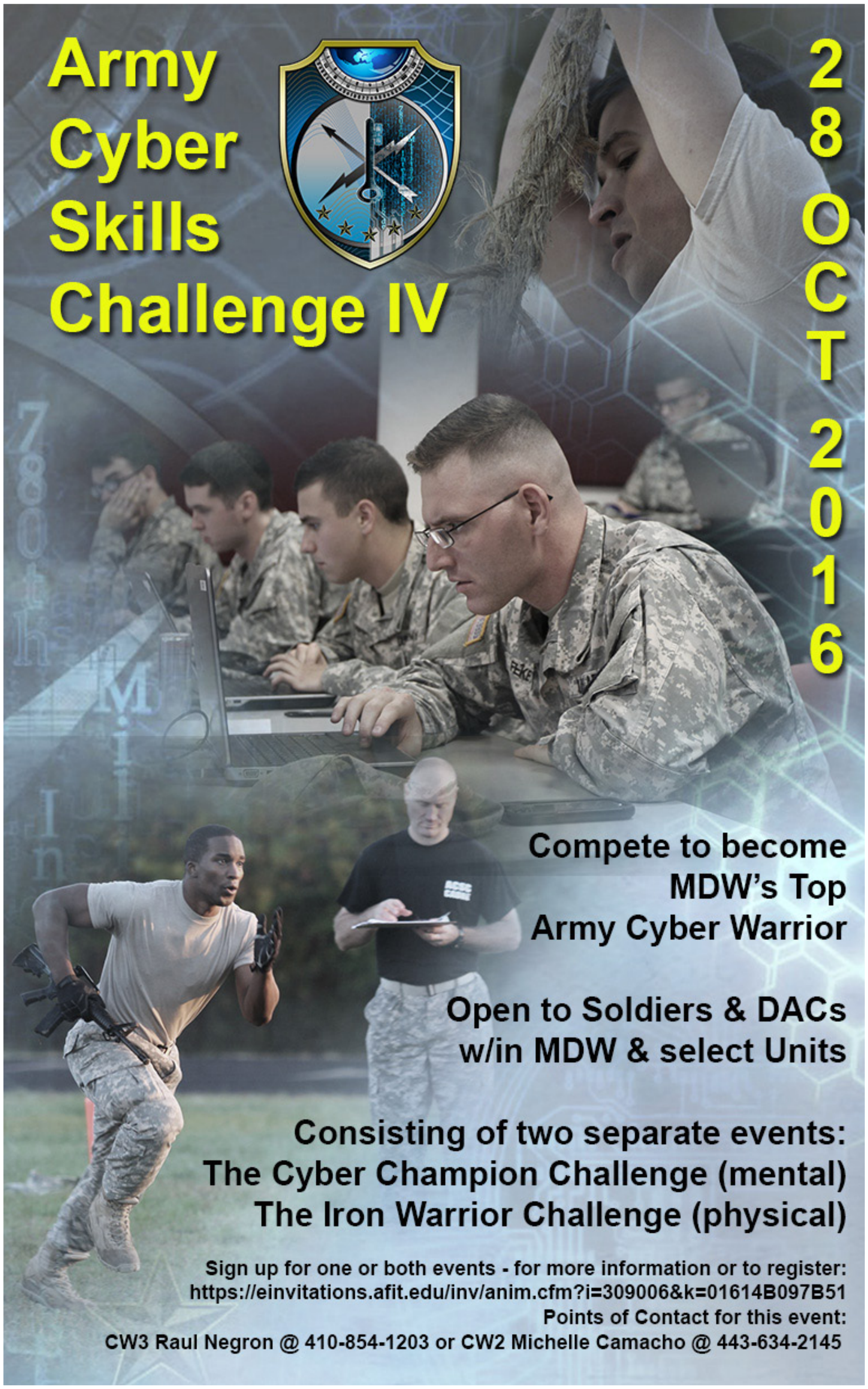
from the past, preserved when the words were not erased, and then became part of the office. Retired CW3 Scott Brown wrote "You are my sunshine, my only sunshine … you make me happy when my beer is warm … you will never know just, how much I like you … please don't take my O'Reilly away!" in reference to the second, and longest serving, Brigade STA – CW5 John O'Reilly. John, if you're reading this, just know that at least your name remains in the room!



- Hanging on the front of the desk is a plaque with the design from the Task Force Echo Shoulder Sleeve Insignia on it, and a piece of server hardware mounted to it, made by Army National Guard Soldiers (including WOs) to commemorate the ten generations of teams that operated critical infrastructure in the building.



- One of the coins on display on the desk is from the July 9, 2004 ceremony on Fort Meade that retired the Eagle Rising branch insignia for the Warrant Officer branch of the Army. This signaled the moment that the Army integrated Warrant Officers into the basic branches and altered their identity from one united corps into a cohort within the Officer Corps. The Cyber Branch would not be established for more than 10 years.



Army Cyber Skills Challenge IV

28 OCT 2016

Compete to become MDW's Top Army Cyber Warrior

Open to Soldiers & DACs w/in MDW & select Units

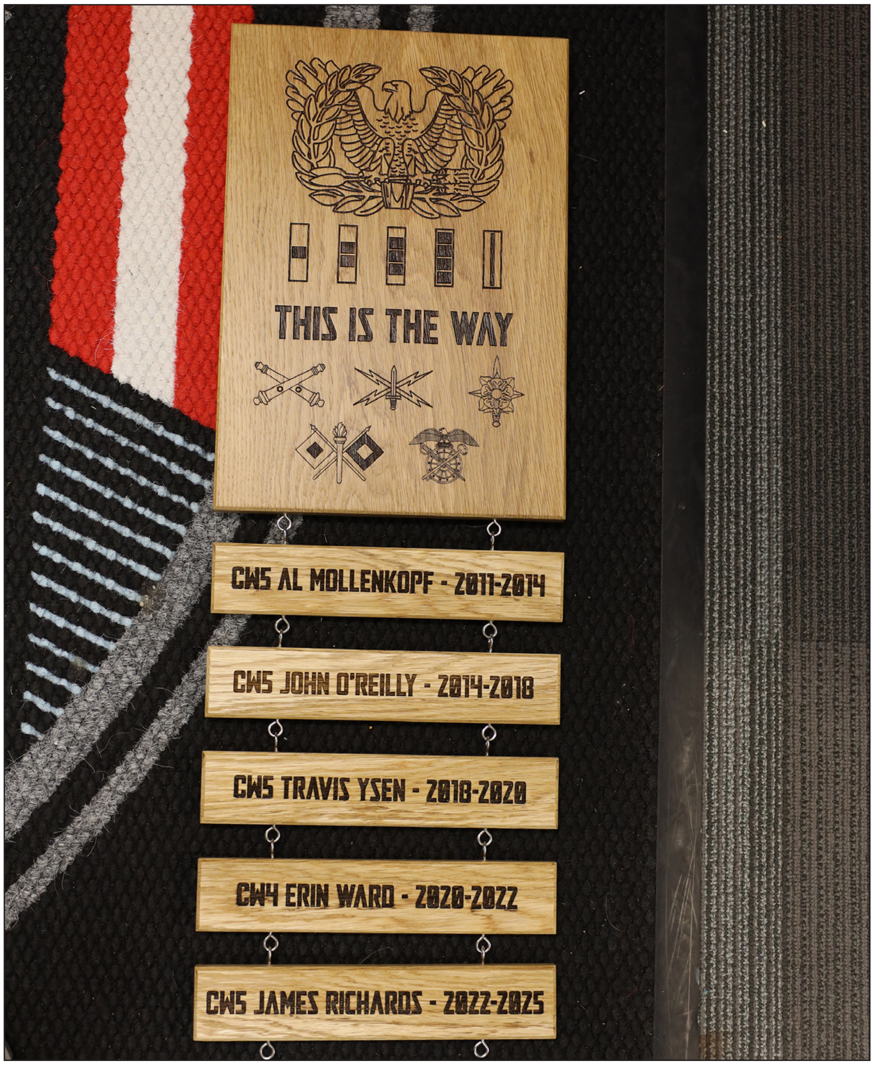
Consisting of two separate events:
The Cyber Champion Challenge (mental)
The Iron Warrior Challenge (physical)

Sign up for one or both events - for more information or to register:
https://einvitations.afit.edu/inv/anim.cfm?i=309006&k=01614B097B51
Points of Contact for this event:
CW3 Raul Negron @ 410-854-1203 or CW2 Michelle Camacho @ 443-634-2145

Like Warrant Officers themselves, the room, artifacts, and the stories inside them are present in the heart of the unit, but at the same time in the background. On August 8, 2024, Retired CW4 Scott Spoor added another artifact – one he made to commemorate the Brigade STAs and CCWOs of the past:

The plaque includes the Eagle Rising – a symbol near and dear to the hearts of the WO Cohort – as well as each of the Army branch insignia that have had WO representation in the Brigade throughout its history. Additionally, under the plaque is a ladder of name hangers with the name of each STA or CCWO, with the years that they served in the position, and was intended to be extended by adding another name to the end as the position endures but the people move on. The backs of some of these hangers have additional information on other positions some of these WOs have held within the Brigade prior to their time as a STA or CCWO. Scott himself served in a number of roles within the Brigade, including a Cyber Mission Force team, a Cyber National Mission Force Team, as one of the first Joint Mission Operations Center SWOs, as a CNMF Task Force Mission Director, and finally in the Brigade Training, Readiness, and Exercises (TREX) section. He remembered the challenges of his time, but it was the legacy of the WO cohort's contribution to the unit and mission that inspired him to help keep it alive with woodworking and laser engraving skills he developed after his retirement.

Part of Warrant Officers' identity is their long tenure in the Army, and with it comes the memory of that tenure. While Room 118 is an interesting place, and if you visit you can usually get the old CCWO talking about an WO story, tracing the cohort's history through artifacts is just the edge of a deep and rich legacy being built by WOs working in their teams or sections every day. WOs are not always the most social people, but if you ask them about their work, you may be able to get a perspective from a witness to history as well as a view into the WO legacy as it is being made. ■


THIS IS THE WAY
CW5 AL MOLLENKOPF - 2011-2014
CW5 JOHN O'REILLY - 2014-2018
CW5 TRAVIS YSEN - 2018-2020
CW4 ERIN WARD - 2020-2022
CW5 JAMES RICHARDS - 2022-2025

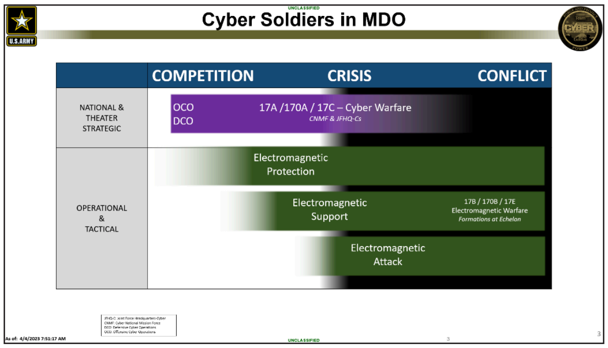
Visions of a Future Warrant Officer

By Chief Warrant Officer 5 Travis Ysen, U.S. Army Cyber Command Senior Electronic Warfare Technician

WHEN I WAS CHIEF WARRANT OFFICER OF THE BRANCH, from the Fall of 2020 to a few months ago, one of the things I tried very hard to shape was the way a new Cyber Warrant Officer looked at their future. After many conversations with the newest members of our cohort, I started writing down the vision I was trying to convey, ultimately making a "welcome letter" of sorts. This is the identity I hoped that our newly appointed members would take on, if not right away, at least over time. A lot of the articles in this issue talk about a Warrant Officer's identity retrospectively – my welcome letter is what I would have liked to get at the beginning of the journey.

Dear Newly Appointed Warrant Officers,

Congratulations on your decision and ultimate selection to become 170A/170B Warrant Officers! This decision should rank high on your list of, "Good things I decided to do while in the Army." Also, to your benefit, both Cyber and EW are high focus/growth areas across the Army and the greater DoD. So, you won't find yourself in a position of not knowing your value or lack opportunity to contribute to the mission.



UNCLASSIFIED

Cyber Soldiers in MDO

	COMPETITION	CRISIS	CONFLICT
NATIONAL & THEATER STRATEGIC	OCO DCO	17A /170A / 17C – Cyber Warfare *CNMF & JFHQ-Cs*	
OPERATIONAL & TACTICAL	Electromagnetic Protection		
	Electromagnetic Support		17B / 170B / 17E Electromagnetic Warfare *Formations at Echelon*
		Electromagnetic Attack	

JFHQ-C: Joint Force Headquarters-Cyber
CNMF: Cyber National Mission Force
DCO: Defensive Cyber Operations
OCO: Offensive Cyber Operations

As of: 4/4/2023 7:51:17 AM

UNCLASSIFIED

3

To highlight the roles of the 170A and 170B, the Cyber School uses the chart above to provide context of the degree of participation that is expected from each MOS throughout MDO. Generally speaking, 170As will be heavily engaged throughout competition and crisis – the main effort is to keep us in competition to the greatest extent possible. That's not to say that 170As won't have a role during conflict as there are several variables to consider, but it will likely be much less when compared to the previous phases. 170Bs on the other hand will become more active as we cross from crisis to conflict. This is due to their role in detecting, identifying, locating, and affecting targets within the electromagnetic spectrum (EMS) while protecting our assets and personnel from enemy/friendly EMS effects. The 170Bs' main efforts are tied to planning, targeting, and effecting the adversary's ability to effectively communicate, sense, and understand the situation as presented in and through the EMS. With that said, both MOSs offer a lot in regard to career growth and personal fulfillment from a professionalization and technical standpoint – the sky is the limit (or is it?)!

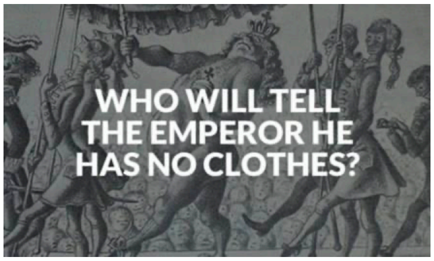
There are a number of things that will be expected of you upon awarding of 170A or 170B (don't worry, this is nothing new):

1. As a Warrant Officer, you are expected to be a technical expert within your field. Having been selected as a Warrant Officer, you have already proven yourself to have a solid technical foundation and high potential for expanded responsibilities. While the intent of WOBC and follow-on PME is designed to increase your technical ability, true expertise in your field will take dedicated effort, continuous learning, and time. Keep an eye on the horizon line for emerging technologies, tactics, techniques, and practices that our operational force needs to be aware of and adapt to or overcome as the mission requires. I am confident that none of this is news to you, otherwise you wouldn't be where you are today.

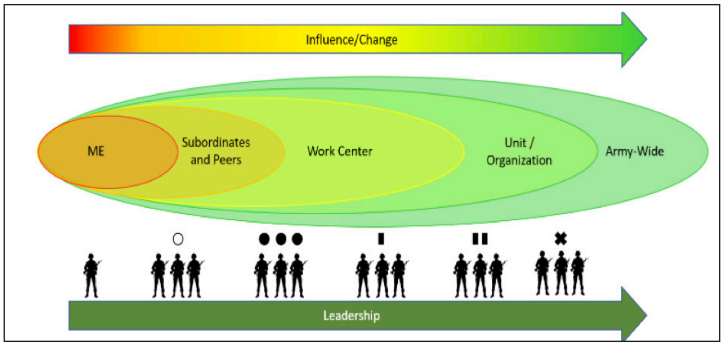
I NEED TRAINING TO USE OUR NEW SOFTWARE.
PRETEND WE HAVE A JOB OPENING FOR A TECHNICAL EXPERT IN THAT FIELD. THEN ASK APPLICANTS HOW THEY WOULD DO WHATEVER IT IS THAT YOU NEED TO DO.
DOES YOUR COMPANY PROVIDE TRAINING?
"PROVIDE" IS A STRONG WORD.
Dilbert.com DilbertCartoonist@gmail.com
4-2-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.

2. As a Warrant Officer, you are a trainer, mentor, and leader. Yes, all those lessons about training, mentoring, and leading as an Enlisted member carry over to the Warrant Officer cohort. As technicians, your leadership role is slightly different than that of your Enlisted and Officer counterparts. Your primary role is to focus on enabling the mission to progress in the right direction which requires technical acumen, humbleness to learn from others and mistakes, and drive/determination to keep positive momentum. You should always be looking to help improve your subordinates and peers in an effort to elevate the team's capability which will further the mission. Sometimes, this will be in the form of developing training, updating an SOP or JQR, or providing one-on-one coaching and training to ensure a concept, process, or policy is understood. Other times, it may lean more into traditional leadership/mentorship where you help someone through a professional or personal challenge. In other words - it's a

3. As a Warrant Officer, you are expected to provide honest, constructive feedback across a wide range of situations. Sometimes this can be uncomfortable; also this role is not meant to be used as a weapon! It is our role as Warrant Officers to identify deficiencies, formulate potential courses of action, provide recommendations, and implement the decisions made as best we can. Learning to do this in a manner that doesn't offend or create rifts can be a challenge – it takes practice!



4. As a Warrant Officer, you are an agent of change. Now that you have made one of the best decisions in you Army career (remember – it's on your list!), it's time to start thinking about the changes you want to be a part of in the coming years. This will take influence which is linked to leadership which is further linked to technical acumen, work performance, and character. While it is true that Warrant Officers need to build technical depth within a trade, they should also grow breadth as they advance in experience and rank which enables influence; this will mean you may need to jump out of your comfort zone to some degree within your career. By continuing down the path that you established already, much of this should come somewhat naturally.



5. In conclusion – each of you should be proud of yourselves for having progressed to this point in your career. You have done well – keep up the great work and momentum as you enter this next phase of your Army career. I look forward to seeing you out in the force and the positive impact that you will have in the coming years!

**Don't worry, as WO1/CW2, you need to focus on building depth within your skill set.*

Identity over time

By Chief Warrant Officer 4 Chad Mastbergen, STA, Operations Support Element, 780th Military Intelligence Brigade (Cyber)

THERE ARE PEOPLE WHO HAVE SPENT ENTIRE LIFETIMES studying sense-of-self, collective identity, self-identity as well as other related concepts in psychology and philosophy all in an in the attempt to understand "who am I". In simple terms identity is what distinguishes one person or item from another. A person's identity is in constant state of evolution, that is not typically given much thought.

I personally have adopted that a person's reality is the product of perspective times experience. [Reality=(Perspective) Experience] You can change your perspective but can only gain experience over time. This concept has allowed me to rationalize thoughts on how identities evolve over time. An individual's overall identity is made up of smaller pieces such as self-concept, Army Identity, and Warrant Identity, as well as countless others depending on how you want to divide up influences. The same experiences are building blocks for both identity and reality but can be utilized in different ways to help construct the complex web that builds each person into what they currently are. A block may be much more than a simple block, when viewed from a different perspective or in its entirety.

The transition to Warrant Officer is a significant life event, that requires a different perspective. Warrant Officers are subject matter experts in a given specialty field. Ideally, they are selected from the top 10 percent of the top 10 percent of the specialty. Chief is expected to have the answer to the question, regardless of if you are a new WO1 or a CW5 with 25+ years of service.

How you perceive and approach a problem is different as a Warrant Officer. You should not only be looking at an immediate solution but also how to solve the problem in the long term, so it doesn't have to be continually revisited. This necessitates you needing to be able to shift your perception of the situation to different points in both the process and different times to enable a more comprehensive understanding of the situation. The ability to conceptualize the greater idea in both time and space from multiple perspectives is extremely beneficial.

Time as a WO1 is typically split between trying to be the very best at your craft and coming to grips with the expectations that you now have as a Warrant Officer. By CW2 there is greater understanding of what is expected of you as a Warrant Officer, but there is still a drive to be the very best at your craft. CW3 is very distinct transition point in a career it is less about how you as an individual can be the best at your craft and more about how Chief can help improve the organization and processes. At CW4, you are taking care of the young Warrants following you up the ranks, very likely in a billet where you are a direct advisor to a BN or above Commander that is making decisions. CW4 also seems to be the time in a career that "how the Big Army runs" enlightenment seems to happen. CW5, the lightsaber wielding mythical creature, they do exist. The CW5s are advising the General Officers helping shape the pathways of future generations. This is a generalized concept, and everyone's experience will vary.

The evolution is continuous but there are still tidbits that can help shape your identity and perspective.

- Be humble, everyone knows something that you don't.
- Learn from everyone, even the people that are not good at things.
- Empower your people, you aren't the only capable person.
- Document your processes and expectations.
- Think "what happens" if you aren't there.

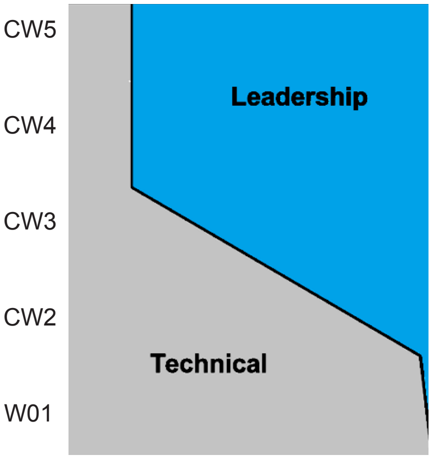
Identity and how it evolves over time is inherently interlaced with experience and perspective. Everyone's journey will be personalized based on their unique experiences and viewpoints. The question is what are your identities at the current time? (perspective reference chart included). ■

On a scale of Meow, what is your Identity today?

The Warrant Officer's Identity as a Battalion Senior Technical Advisor

By Chief Warrant Officer 4 Nolan Reed, Senior Technical Advisor, 782d Military Intelligence Battalion (Cyber)

SECTION 4-9 OF THE 2023 VERSION OF DA PAM 600-3 DEFINES A WARRANT OFFICER as "a technical expert, combat leader, trainer, and advisor. Through assignment experience, training, and education, the WO administers, manages, maintains, operates, and integrates Army systems and equipment across unified land operations." If we continue reading, section 4-9 b. (3) tells us that a Chief Warrant Officer 4 (CW4) is a "senior-level technical and tactical experts who perform the duties of technical leader, manager, maintainer, sustainer, integrator, and advisor and serve in a wide variety of branch-level positions." The key words to take note of within that definition for a CW4 are "and serve in a wide variety of branch-level positions."



Many of us have seen a version of the Technical-Leadership focus transition-by-rank diagram. This diagram shows us that as we progress in our careers, our focus shifts from being almost exclusively focused on our technical prowess to more of a leadership role. Within Cyber, we can ignore this (to an extent), as we have W4 positions within our teams. These individuals can maintain most of their focus on their technical craft.

Aside from HRC Career Manager, the Battalion Senior Technical Advisor (STA) is the first position with most of its focus within the leadership spectrum. As the BN STA, we are a part of the BN Command Team and serve as one of the Battalion Commander's most trusted advisors. Within our technical sphere, we oversee our collective training events and the BN Assessor pools. We review and approve or deny exceptions to policy requests for JQR (Joint Qualifications Requirements) completion. We provide guidance and recommendations to ensure the supported OPCON HQs are getting what they need from our teams, and to work with them in finding solutions to JQR/JQS (Joint Qualification Standard) completion problems. We help troubleshoot systems, conduct data analysis, and find and test new pieces of equipment and technology. We are also the touchpoint at the battalion level for JQR review and updating, which then feed into the Brigade and U.S. Army Cyber Command work role working groups.

Beyond these technical responsibilities (and more), the BN STA also serves as the BN's Senior Warrant Officer Advisor (SWOA). MILPER Number: 23-399 defines the requirements, role, and responsibilities of this "additional duty". In this capacity, we truly "provide leader development, mentorship, and counsel to other warrant officers, officers, NCOs, and Army civilians" that previous versions of DA Pam 600-3 defined. As the SWOA we are responsible for providing operational advice to all cohorts. More heavily though, we are now responsible for providing career mentorship and counseling to other 170As, 170Bs, 131As, 352Ns, 255Ss, and 170Ds. We provide our commander with OER (Officer Evaluation Report) enumeration recommendations and senior rater comments, while also ensuring that the rater's portion accurately reflects the rated Warrant Officer's performance. We advise the commander on the performance, training, conduct, force management, and talent management of the organization's warrant officers.

With over 700 personnel, approximately 70 of whom are Warrant Officers, spread across three states, most of my time as the 782d MI BN STA is focused on my SWOA responsibilities. In the 781st MI BN (Cyber), at a smaller size and supporting only one OPCON HQ, the STA-SWOA balance tips more toward the technical advisor side. Within the 11th Cyber BN, as the Army's only organic expeditionary cyber battalion, its STA faces unique challenges. The 11th's STA must not only be a technical SME in their MOS (170A or 170B) and be able to coach and mentor the other members of the organization, but they must also become an expert in the other MOS to fully understand what their teams should be doing and need. The 11th does something else that neither the 781st nor 782d do, they go to the field and deploy, which adds another layer of complexity.

While staying on a team is an option for our CW4s, taking on the role of the BN STA is something that members of the Army's centralized promotion boards understand, and historically pushes these individuals higher in the OML than their strictly technical counterparts.

So, if your STA always looks busy, and you must send a calendar invite to ensure you get some face time with them, know that we are constantly in motion serving you. We attend meetings that we'd rather skip to ensure that you are taken care of. We advise the commander, and the Team leads to the best of our ability. You are at the heart of everything that we do. ■

Being Chief

By Chief Warrant Officer 4 JP Dixon, J38 Mission Director, U.S. Cyber Command

BEING CHIEF HAS DEFINED AT LEAST HALF MY CAREER at this point. It is not always easy. Sometimes it demands more than a person wants to give. Sometimes it demands doing things you did not know you were capable of and sometimes it feels overconfident or even arrogant to be able to say, "I'm the Chief, I got this". All that said, it is almost always incredibly satisfying. It took me a long time to join the illustrious Warrant Officer cohort. This is how I got there.

The first time I ever worked with a Warrant Officer I was a new Staff Sergeant leading a section on the watch floor in Hawaii responsible for supporting force protection and tracking strategic weapons deployments in the INDOPACOM area of operations. He was the deputy chief of the division level organization we belonged to. Our interactions were sparse and I didn't hear much from him. He kept day hours essentially performing management functions while I worked long shifts, leading and directing day-to-day ops and real-time actions to support our mission and objectives. Frankly, I wasn't impressed. Warrant Officer recruiting briefs came and went without catching my attention because I loved what I was doing and got to see the results in real time when my team's work make a difference. I didn't think about him, what he did, and what was different about being chief then.

My next duty station was different. My new boss was a retired Chief. He was more than a boss though, he was a fully engaged leader and mentor. He was as invested in his people as his mission and aside from "keeping the wheels on the bus", he consistently sought to improve our ability to perform our mission by advocating for training and opportunities to expand our understanding of what we were doing. He set the new bar for me and helped shape me as a leader. That said, I also had the additional duty of being Platoon Sergeant during that time to about thirty Soldiers, a few Chiefs among them. They were experts in their sections, but they rarely stood out for me. They were always friendly and professional. They were rarely ever at formation or PT. I didn't see it then, but they were those same kind of leaders as my mentor, they just didn't work to extend their influence beyond the shops they worked in.

Iraq was where I really learned the value of being Chief. I was deployed as part of a small team with two primary roles. My first duty was to serve as the in-country expert and teach deployed collectors and analysts how to find the enemy in the data we collected, to in turn support what would become the "Find, Fix, Finish" targeting model. Second, was to pursue high priority targets and solve hard problems within the area of operations as part of a team. In those two roles I was able to interact and work closely with several Warrants, ranging from deployed team and section leads to the Multi-National Force and Corps senior advisors. I was able to see how those Chiefs led their troops and advised their leaders. They made a difference everywhere they were. I was exposed to the Chiefs I think of now as "legends", the ones who were shaping the future leaders, organizations, policies, and technologies used to accomplish our missions. These were the kind of leaders I wanted to be and they stayed in or connected to the operational community for most of their careers.

Despite my newfound respect and appreciation for what it meant to be Chief, I came home to do those same things in garrison that I loved down range, so I didn't pursue that first spot right away. I was teaching and developing new technology and analytics to support ops. It wasn't until I reached the point where the Army asked me to take a company and stand in as First Sergeant that I realized I had to decide about my future. I could still be the leader I wanted if I stayed enlisted, but I wouldn't be able to keep doing the same jobs I loved. Then the Army interrupted all that deep planning with a nominal assignment that kept my family stable, so I took it and went to the Joint Staff. I walked in the door and told my new boss my plan. I would stay on his team and serve my time, but I was putting in my packet and planned to leave there as a Warrant Officer.

From there I learned some other lessons and had many great mentors, both deployed and back in garrison. I learned that those spots meant instant and implied trustworthiness and expertise. I also learned that it was my responsibility not to tarnish that reputation. I enjoyed open door access to Commanders and General Officers anytime I needed it, mainly because they knew I wouldn't abuse it and because when I came to them it was important. Earning those dots opened the door for me to try and keep making a difference and to broaden my influence. I can honestly say I at least feel like I have made a difference, whether it was taking insider and insurgent threats and "high-value-targets" off the field, helping to identify strategic threats and issues for national leaders to engage, or developing new leaders, new tech, improving policy. Most important has probably been teaching new generations of Soldiers, Sailors, Airmen and Marines about what we do and why we do it. Those wins did not come without loss and hurt. There have been enough lessons learned, some paid for with lives, that identified critical gaps or flaws in how we do things. One can't help but feel like we should have done better, and must keep trying to do better to prevent future losses. We owe them our best efforts to not make those mistakes or miss the things that might have prevented their loss. That responsibility cuts deep. Overall, with the wins and the losses along the way, being Chief has been and remains one of the greatest honors in my life. As a Warrant, I'm part of a cohort that is more like a team and sometimes like a family. We share our love of the service and the mission as we also share our knowledge to get things done. ■

Empowering Citizen Soldiers: Mentorship Approaches for National Guard and Reserve Soldiers

By Chief Warrant Officer 3 Nefertiti C. Stokes and Chief Warrant Officer 4 Adam D. Crenshaw, Task Force Echo VIII and 126th Cyber Protection Battalion

THE AUTHORS OF THIS ARTICLE ARE BOTH MEMBERS OF THE NATIONAL GUARD and served together during a 400-day deployment as part of Task Force Echo. During the deployment, both officers collaborated on Warrant Officer Professional Development (WOPD) engagements. They identified the unique gaps in effectively providing mentorship to the National Guard and Reservist in comparison to the Active Component. Effective mentorship is of utmost importance in the dynamic and challenging environments of both military and civilian life. A broad mentorship program that enhances both Military and civilian careers would be an exceptionally effective tool for developing outstanding leaders. Mentorship facilitates professional advancement and fosters personal maturation, fortitude, and preparedness. Influential mentors significantly influence the early promotion of junior officers in the US Army, particularly for highly capable mentees, and when the mentorship lasts longer (Lyle & Smith, 2014). This paper seeks to introduce a mentorship structure that specifically caters to the mentoring requirements of National Guard and Reserve component Service Members, both in their military and civilian professions. This approach aims to follow the well-known example that National Guard and Reservists have shown by balancing their military and civilian careers: being good at one makes them better at the other.

It is vital for military readiness to foster a culture of continuous learning and development and provide a structured path for career advancement and personal fulfillment. Professional development sometimes happens sporadically and without a clear connection, often impacted or interrupted by operational demands and assignment schedules (Jackson, 2018). Additionally, it needs the guidance of experienced professionals. Mentorship becomes even more complex for National Guard and Reservist part-time soldiers, who balance military commitments with civilian careers (Kirchner & Herd, 2021). Many established mentoring programs currently exist, albeit in siloed organizations. Programs such as Army Career Tracker and the Center for Army Leadership allow Soldiers to create an Individual Development Plan (IDP) (Army Career Tracker, n.d., Center for Army Leadership, n.d.). This provides an incredible source for Military personnel to connect with leaders in their field. It is designed to match a Soldier's career progression whether serving on active duty in the U.S. Army Reserve (USAR) or Army National Guard (AR 600-100, 2017). However, it still caters more towards active duty personnel. Another program which caters to civilian professional engagement is from the United States Army Training and Doctrine Command (TRADOC). They aim to deliver expert civilian human resource consultation throughout the career lifecycle of Army Civilian Professionals (Mentoring Portal – U.S. TRADOC, n.d.). Even though these and other training programs offer distinct and substantive collaboration opportunities, they do not address the competing priorities of National Guard and Reserve Service Members.

Becoming a mentee offers many advantages for personal and professional development. A key benefit is the tailored guidance and support from an experienced mentor who can provide insights based on their career journey. Mentors help mentees acquire new skills, enhance existing ones, and open doors to valuable networking opportunities that can accelerate career advancement. Moreover, mentorship fosters personal growth by building confidence, managing stress, and achieving a healthy work-life balance. Feedback and accountability from a mentor are vital for setting and achieving goals, while their broader perspectives can help mentees navigate challenges more effectively.

Choosing the right mentor involves a thoughtful process that begins with clearly defining your goals and needs. Potential mentors should be identified within your network or industry, ensuring they possess relevant expertise and experience. Evaluating their track record of successful mentorship and ensuring compatibility in communication style, values, and personality is essential to establishing a productive relationship. Building trust and maintaining regular communication is crucial for a successful mentorship, as well as being open to feedback and adjusting the relationship as your needs evolve.

The following are concise mentoring session topics that will facilitate a structured and successful mentoring experience (for access to the workbook they developed, please reach out to the authors):

Individual Development Plan (IDP)

An IDP is essential for structured and effective personal and professional growth. An IDP provides a clear framework for identifying and achieving specific career goals, ensuring that individuals can strategically plan their development in alignment with their personal aspirations and organizational objectives (Army Mentorship Handbook, 2005). By outlining specific skills to be acquired, competencies to be enhanced, and milestones to be achieved, an IDP helps individuals maintain focus and motivation. This structured approach clarifies the path to success and makes it easier to track progress and make adjustments as necessary, ensuring continuous and targeted development.

Emotional intelligence (EI)

EI is crucial in personal and professional contexts as it enhances self-awareness, self-regulation, and empathy. In personal life, EI helps individuals understand and manage their emotions, leading to better mental health and stronger relationships. Emotional intelligence is perceiving, using, understanding, and managing emotions effectively (Chin et al., 2015). Professionally, it is vital for effective leadership, as it enables leaders to inspire and motivate their teams, handle stress, and manage conflicts efficiently (Salovey et al., 2005). High EI contributes to improved communication, reduced stress, and more meaningful interactions, fostering personal growth and professional success. Effective leadership depends on emotional intelligence (EI), which combines the capacity to recognize, control, and use emotions in others and oneself. High EI leaders are skilled in self-awareness; they can identify their emotional states and how they affect their conduct and decision-making. They show self-regulation, control, and flexibility even under challenging circumstances. These leaders also empathize and can recognize and meet their subordinates' emotional requirements, creating motivating surroundings. They also shine in social skills, developing close bonds, deft conflict resolution, and motivating and steering their groups toward common objectives. Emotional intelligence improves a leader's ability to relate to people, propel favorable results, and build a solid corporate culture.

Technical Acumen:

Technical acumen refers to a deep understanding and proficiency in using technology and technical concepts (Ng, 2007). It encompasses the skills, knowledge, and ability to apply technological solutions effectively. This allows us to solve problems, optimize processes, and innovate within a given field. According to Schunn & Silk (2011), technical acumen is not limited to IT professionals; it is valuable in various industries where technology plays a significant role. Leaders must have the technical aptitude to grasp and use technology to propel operational effectiveness and innovation. Strong technological abilities enable leaders to interact with technical teams and make informed decisions properly. Moreover, technically competent leaders can encourage a culture of constant learning and adaptation. Technical knowledge ultimately helps leaders to have the insights required to match technical capacity with strategic objectives, promoting success and sustainable development.

Military Professional

The professional development of a Service Member should focus on advancing technical skills, leadership capabilities, and strategic thinking. As leaders, understanding Multi-Domain Operations (MDO) and Large Scale Combat Operations (LSCO) is crucial for effectively contributing to modern military strategies. MDO involves integrating and

synchronizing capabilities across various domains—land, sea, air, space, and cyber—to achieve strategic objectives. It requires a comprehensive understanding of how these domains interconnect and impact each other. LSCO, on the other hand, refers to high-intensity warfare involving large formations of troops and complex operations across extensive battlefields. It necessitates proficiency in planning, coordination, and execution of large-scale maneuvers. For a National Guard or Reservist, understanding MDO and LSCO means being prepared to integrate and operate across multiple domains in coordination with active-duty forces. It involves developing complex skills and ensuring readiness for rapid mobilizations. This preparation enhances their ability to support national defense strategies and respond effectively to domestic and international missions.

Another critical focus is the Army Officer/Non-Commissioned Evaluation Report (OER/NCOER) and the Officer/Enlisted Record Brief (ORB/ERB). These are essential tools in a leader's career management and development. The OER/NCOER comprehensively assesses performance, potential, and leadership abilities. It is critical for promotions, assignments, and professional development opportunities. It ensures that leaders are evaluated fairly and consistently, reflecting their contributions and competencies. The ORB/ERB, on the other hand, is a This is a snapshot of the leader's career. It provides details on their qualifications, assignments, education, and other relevant information. These documents play a pivotal role in shaping a leader's career trajectory.

Civilian Professional

Balancing a Military career with a civilian career presents unique challenges and opportunities. National Guard and Reservist members must navigate dual roles, managing responsibilities in both military and civilian spheres. Understanding the key factors influencing this balance can help service members, employers, and policymakers support these dual-career individuals effectively (Kirchner & Herd, 2021). Balancing a National Guard/Reservist and civilian career requires navigating dual identities, managing mental health, and leveraging support systems. Legal protections and employer support are crucial in ensuring that National Guard members can successfully integrate their military and civilian responsibilities, benefiting their personal and professional lives.

Career advancement is affected by many things, such as personal traits, support from the company, and outside circumstances. By understanding these factors, people and businesses can advance their careers more quickly. Over the last few decades, early career advancement has stayed the same. However, pay and job advancement have changed depending on the industry and job (Keiller et al., 2020). Developing a comprehensive plan for civilian professional development from six months to five years will significantly enhance career outcomes. Working a civilian career parallel to a military career can provide much complexity. In a study conducted in the United Kingdom, Whybrow and Milligan (2021) identified that while transferable abilities might help in civilian employment, veterans may undervalue their military experience, and it can be challenging to adjust to corporate standards. It is also important to note that personality traits significantly influence both intrinsic satisfaction and extrinsic success during a career. Career advancement is heavily influenced by personality, education, and industry, with those who advance more quickly tend to have comparable features and attributes (Pan et al., 2017).

Leadership

Leadership development is a critical aspect of organizational growth and success. Leadership is the activity of influencing people by providing purpose, direction, and motivation to accomplish the mission and improve the organization (ADP 6-22, Army Leadership and The Profession, 2019). Effective leadership development programs can enhance leadership skills, improve organizational performance, and prepare individuals for future leadership roles. Leadership development should bridge the gap between leader and leadership development, emphasizing human and social capital creation in organizations (Day, 2000). Both military and civilian leadership require a blend of technical skills, interpersonal abilities, and strategic thinking. While the contexts may differ, the core competencies of effective communication, adaptability, and the ability to lead under pressure are crucial for success in both domains. The Be-Know-Do framework effectively develops leadership attributes and competencies, leading to improved organizational results through the people they lead (Henderson, 2023). These concepts help build leadership capital. Leadership capital refers to the reservoir of trust, goodwill, and influence a leader accumulates and can draw upon to mobilize and inspire their team or organization (Al-Nasour & Najm, 2020). This capital is built through consistent, transparent, and ethical behavior, effective communication, and demonstrating competence and reliability over time. It enables leaders to effectively drive change, make difficult decisions, and navigate challenges by leveraging the credibility and respect they have earned. The stronger a leader's capital, the more adept they are at fostering collaboration, innovation, and resilience within their organization. Overall, integrating structured training programs and focusing on interpersonal skills can enhance leadership capabilities across sectors.

Mental Wellbeing

Mental well-being plays a critical role in military and civilian life, significantly impacting the overall quality of life, productivity, and social relationships. In the military, mental well-being is essential for the effectiveness of service members, as it affects their readiness, morale, and ability to perform under stress. Studies have shown that psychological capital, work satisfaction, and health perception strongly predict psychological well-being in military personnel (Hernández-Varas et al., 2019). Moreover, transitioning from military to civilian life can present challenges to mental well-being, with veterans often facing increased risks of social exclusion and ongoing health issues if not adequately supported (Oster et al., 2017).

For civilians, mental well-being is equally important, influencing workplace productivity and societal health. Promoting mental health in civilian environments enhances the working atmosphere and benefits both employers and employees. Initiatives such as mental health programs can improve job satisfaction, reduce stress, and lower absenteeism, leading to better overall performance (Hartwell, 2015). The emphasis on mental health across various sectors underscores its universal importance and highlights the need for effective support systems in both military and civilian settings.

Integrating mental well-being strategies across both military and civilian life is essential, as each domain can impact the other. Effective support systems in one area can positively influence the other, enhancing overall well-being and performance. Addressing mental health proactively in both contexts ensures that individuals can navigate the complexities of their dual roles—balancing military duties with civilian responsibilities—and maintain optimal performance and quality of life in both spheres.

Conclusion

Mentoring National Guard and Reserves members is crucial for developing their leadership capabilities in both civilian and military contexts. Effective mentoring programs can bridge the gap between military discipline and civilian career aspirations. This, in turn, provides service members with the skills and confidence needed to excel in diverse environments. By leveraging the unique experiences and challenges National Guard and Reserve members face, mentors can offer tailored guidance that enhances decision-making. This dual-focused mentoring prepares these individuals for leadership roles within the military and equips them with the competencies required to thrive in civilian careers, fostering a seamless integration of their dual responsibilities.

Furthermore, structured mentoring relationships can help National Guard and Reserve members navigate the complexities of balancing military service with civilian employment. Mentors can provide insights into effective time management, stress resilience, and career development strategies, ensuring that mentees can maintain high performance across both spheres. By fostering a supportive and knowledgeable network, mentoring programs contribute to service members' personal and professional growth, ultimately benefiting both the military and civilian sectors. This holistic approach to leadership development underscores the value of mentorship in cultivating well-rounded leaders who can adeptly handle the demands of their dual roles.

I’d Rather Be Me

By Chief Warrant Officer 3 Jason Ehlinger, Chief Operations Technician, 781st Military Intelligence Battalion (Cyber)

HALF MY LIFE AGO, I SAW A DIFFERENT PATH FOR MYSELF. I was an art student, and it only took a year of that for me to see it for what it was, a worthwhile passion but worthless as a career. Pretty shocking stuff, I know. After that freshman year, I was uncertain as to what to do with my life and wanted to make anything for myself, so I joined the Army. Here, nineteen years into an indefinite career, I do not regret briefly pursuing my passion as an artist because my creative side will always be a big part of who I am.

My career thus far is nearly half and half SIGINT and Cyber. The combination of these was lots of training on analytics and logic. I was made to memorize some Morse. The Colonel works like that. No not that Colonel this kernel. What does that port do? No, the one with the ships not the one open on 9001. Well, you can try to put the guhor stick in the USB slot but I assure you it does not work like that. Yes, you could guhor a net map, but this is CYBERCOM in 2024 please use technology. But really, at each duty assignment, combining my creative side into the mix tends to be far more useful than my logical/analytical side alone.

Many times, I have fallen into a duty position that is truly stagnant. I cannot fault those who came before me. They are executing exactly as expected and depending on the OPTEMPO are likely very, very tired. Task, condition, standard. Crawl, walk, run. Repeat. Repeat. Repeat. PCS to circumvent burnout (maybe). Repeat. Repeat. Repeat. This is how the military functions and it works, and, for most people, a career can be done this way. I get bored though.

Without any strict structure, I pursue each duty assignment in a similar way. What is the work required? What can make it faster, more complete, better? Cleaning that up frees time to get more creative, find a shortcoming, an inefficiency, a flaw, and make it better. I dislike busy work, but certain things just need doing. Optimizing the busy work lets me really look at what can improve the mission set. I see breaking the mold as an expression of my artistic side. I was given a job, but what can I make of it?

When I was enlisted, I was still me, optimizing, breaking, remaking, and it was valued by the Army as evidenced by steady promotions. As a Senior NCO, looking at applying for Warrant Officer or trying for the next Enlisted rank, I could see that as an Operator, the next Enlisted rank wouldn’t happen for me. Not unless I denied who I like to be as an individual. The gooey ephemeral problem solver. Also, a Senior NCO eventually needs to be a people person. That is a weak point for me. Could I overcome it? Probably. Could I let the people more natural at it do that while I do the things they are less natural at? I chose the win-win.

Lots of things I do fail, are lackluster, or reinvent a process to suit my weirdness while questionably adding value. The successes still feel good. Over the years, I’ve gotten feedback like, “you did my whole job in less than twenty minutes,” or, “I open four tabs and know exactly what’s going on,” or, “you bring order to chaos.” I never know how to respond as I was just doing what I always do. Regardless I take it as I am doing something right.

This is, to me, the essence of the Warrant Officer Cohort. Try the weird thing. Break it. Fix it. Learn from it. Teach others. Drive change. Warrant Officers keep it fresh. In this essence I found a way to be myself, the artist, and be in the Army. As for whether this is what the Army wants its Warrants to be, it is hard to say. As an entity, the Army has no one unified voice on the matter. A couple insights come from fun places though, Army recruiting slogans and promotion criteria.

I grew up in the “Be All That You Can Be” era. All in all, it feels like a solid slogan. Kinda wordy but the message is clearly stated, B-tier. The Army recruited me in the “Army of ONE” era. I actually really like this one. Give me a sneaky double entendre and a hint of saloon and I am there. Solid A-tier. Most of my service is the “Army Strong” era. This is C-tier work at best. Shorter is good but this is too short. “Warriors Wanted” era came around after the Army shifted from Warrior Leader Course back to Basic Leader Course and is getting a D-tier for mixed messaging and being nearly instantly replaced because of the mixed messaging. Absolute F-tier for the “What’s Your Warrior?” era. Cringe. My warrior is cringing. Thankfully it looks like we are back to A-tier work with the shorter form “Be All You Can Be” from my youth. Sticking with the passing grades, we have a theme. The U.S. Army projects to the world that it takes strength from the individuals that comprise it.

In the potpourri of contradiction that is the Army, to me, Warrant Officers have the most freedom to express their individuality. The distilled essence of the Enlisted is to follow the orders and regulations they are given. The Army needs its Enlisted ready to die in glorious combat. The distilled essence of Officers is lead. The Army needs its Officers ready to motivate their Soldiers to go die in glorious combat and to render the proper punishments under UCMJ if a Soldier does anything that makes them not ready to die in glorious combat. Individuality is contradictory to those functions. Enter the Warrant Officer. Do we die in combat? Unequivocally yes, bullets and bombs are indiscriminate. But as far back as 1896, the Army’s expressed traces of acknowledgement that it’s kinda good not to have everyone be cannon fodder and master technical tasks that are hard to replace.

We see this echoed in the promotion systems for Enlisted, Officers, and Warrant Officers. Specialist to Sergeant

and Sergeant to Staff Sergeant promotions depend on a face-to-face demonstration of knowledge of regulations performed under pressure. Staff Sergeant to Sergeant First Class and above we see a records check. Each persons' service history is validated against hard and soft criteria on expectations of the next rank. The higher someone goes in the Enlisted ranks, the further they are expected to be from any technical aspect of their MOS. Officers have a very straightforward system; their promotions are functionally automatic up to Captain as long as they don't manage a UCMJ violation. After that the Army wants to see them lead and forces that look via Key Development positions. As it is understood to me, raters and senior raters of personnel in Key Development positions do their most to top block those evaluations so as to not torpedo that person's career, regardless of their actual performance. It is really an extension of the do-not-manage-to-violate-the-UCMJ expectation of the previous ranks. Army Officer MOS generally do not matter for promotion. The Army doesn't value that work from its Officers.

In its Warrant Officer Corp, the Army finally expresses some value in technical expertise in the promotion system. WO1 to CW2 is functionally automatic; do not receive UCMJ and you get promoted on time. Everyone gets at least one this way. The remaining promotions are a records review but with different expectations than for the Enlisted. For my entire time as a Warrant Officer thus far, I managed to stay in deeply technical roles. Based on my evaluations, I seem to have performed them pretty well. This earned me a promotion ahead of my peers evaluated at the same promotion board. On the flip side, I have an Enlisted career twin. Same work role, same certifications, same scope of work. This person is repeatedly passed for promotion.

Getting a little creative with the available data, it doesn't feel like a big stretch that my stomping around and breaking things is what the Army wants its Warrants to do. In this, myself and other art majors that wound up in the Army, get to the core of what really makes the U.S. Army strong. Its individuals. I will hold on to this romanticized view of things until I depart the service. And I plan to depart long before my vision changes to see those I serve with as expendable assets to be managed and not people to be cared for. ■

Targeting in the Cyber Domain (131As)

By Chief Warrant Officer 3 Eric L. Rondeau, Cyber National Mission Force, Joint Task Force Three

"Leave the Artillerymen alone, they are an obstinate lot" – Napoleon Bonaparte.

SINCE ITS ESTABLISHMENT IN 2012, the Cyber Mission Force (CMF) has greatly benefited from the expertise of Field Artillery Targeting Technicians (131As). The majority of 131As serve within the 780th Military Intelligence (MI) Brigade (Cyber), operating at the tactical level across various proficiency levels – Basic, Senior, and Master – in the Fire Support Planner (FSP) Job Qualification Record. These technicians are integral to both National Mission Teams and Combat Mission Teams. Additionally, some 131As are assigned directly to Joint Force Headquarters – Cyber (Army), Cyber Operations – Integrated Planning Elements, and the Cyber National Mission Force.

The expertise of a 131A within the Fires Warfighting Function is rooted in military doctrine and further developed through multi-echelon training and real-world combat experiences in various combatant commands. In 2020, the Deputy Secretary of Defense recognized the importance of the Master FSP position, designating it as a critical billet. In this role, 131As serve as primary technical advisors to CMF Team Leads and Joint Commanders in Joint Targeting.

Targeting Technicians leverage their comprehensive understanding of the Joint Planning Process to develop detailed operational plans and orders for cyberspace operations. They provide expert guidance on the full spectrum of cyberspace effects operations and the Joint Targeting Cycle (JTC). The specialized knowledge and insights of 131As are essential for effectively executing the CMF's mission.

Multi-Layered Approach

As Field Artillery Targeting Technicians, our role within the CMF extends beyond merely targeting entities based on a developed cyberspace capability or established network access. Our mission is to identify and engage targets that align within the objectives of United States Cyber Command (USCYBERCOM) Campaign Operations Orders and Plans, aiming to create deliberate effects. The CMF's operations are not conducted for their own sake; rather, they are guided by a strategic framework, much like the rigor required in lethal targeting. For example, we cannot authorize an MQ-9 Reaper to deploy an AGM-114 Hellfire missile on a suspected target without satisfying a comprehensive set of criteria. The mere presence of an MQ-9 and AGM-114 does not justify their use.

In ensuring that a target aligns with USCYBERCOM's strategic objectives and desired effects, a 131A focuses on challenges distributed across three distinct yet interconnected layers within cyberspace: (1) Physical Networks, (2) Logical Networks, and (3) Cyber-Personas. These layers are integral to shaping our approach to deliberate and effective targeting. They can be loosely associated with the universal computer networking model, the Open Systems Interconnection (OSI) model, providing a structured framework for understanding and addressing the complexities of cyberspace operations.

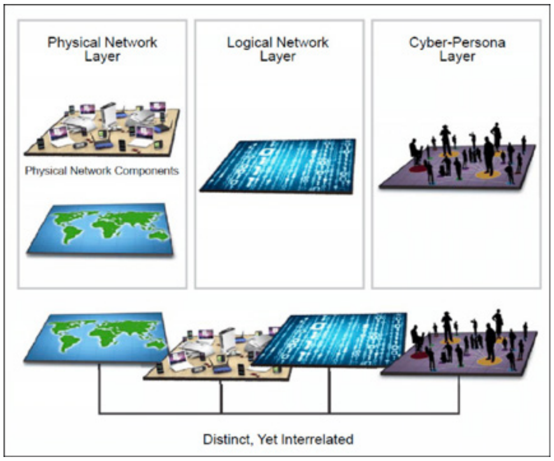


Figure 1. The Three Interrelated Layers of Cyberspace

The Physical Network layer refers to all tangible components that can be physically touched. It corresponds to the Physical and Data Link layers of the OSI model. 131As focus on identifying the geographic location of the entities based on the Physical Network layer. The geographical location will determine the legal frameworks and Rules of Engagement that will apply to ensure that our operations comply with established guidelines and legal constraints.

Moving up, the Logical Network layer abstracts the physical components and corresponds to the OSI model's Network, Transport, and Session layers. Much like the processes of encapsulation and decapsulation in the OSI model, this layer encapsulates more data for 131As to target. The Logical Network layer enables the analysis of Internet Protocol addresses and domains associated with the targeted entities. The more information gathered in the Logical Network layers allows for a more precise and effective approach to cyberspace operations. It is important to note that multiple logical networks can exist within a single physical network. The Logical Network layer is where 131As spend significant time synchronizing efforts to coordinate and deconflict operations between the Department of Defense (DoD), interagency partners, and multinational allies.

The most complex layer, the Cyber-Persona layer, corresponds to the Presentation and Application layers of the OSI model. This layer deals with digital identities, such as profiles on social media platforms, usernames in online forums, and aliases used in encrypted communication channels. Targeting within the Cyber-Persona layer requires detailed insight and intelligence, making it particularly challenging. 131As depend heavily on information professionals to operate within this layer, integrating military information support operations or military deception into cyberspace operations. This nuanced understanding of digital behavior and identity is crucial for effectively addressing targets in the Cyber-Persona layer.

Understanding the Threat

The cyber threat landscape has reached unprecedented volatility, driven by a combination of factors, including the surge in data breaches during the COVID-19 pandemic, the ongoing Russia-Ukraine conflict, and the rapid advancement of new technologies. These conditions have increased various threats, such as Advanced Persistent Threats (APTs), ransomware, social engineering, and malware. These challenges are not limited to the DoD but extend to organizations and governments worldwide. The complexity and ever-evolving nature of the cyber domain makes it increasingly difficult to anticipate and counter these adversaries effectively.

Figure 2. APT29 (Уютный мишка)

A recent example of the persistent danger posed by cyber threat actors is the attack on Microsoft by APT 29 in January 2024. APT 29, known by names such as Midnight Blizzard, Cozy Bear, and Nobelium, is associated with the Russian Foreign Intelligence Service (SVR) and has been a prominent actor in cyber espionage since around 2008. In this attack, APT 29 gained initial access through password spray attacks, compromising user accounts to create, modify, and grant high permissions to OAuth applications. These permissions enabled the attackers to perform malicious activities, including granting themselves the Office 365 Exchange Online "full_access_as_app" role. Leveraging these elevated permissions, APT 29 collected sensitive corporate emails and other intelligence from Microsoft. To evade detection, they utilized residential networks to obscure their traffic. By March 2024, they had compromised the Department of Veterans Affairs account with Microsoft.

As Targeting Technicians in the cyber domain, our role in addressing these threats is crucial and complex. The solution is neither straightforward nor quick. Our work begins with implementing the JTC in USCYBERCOM, a framework that guides cyber threats' identification, prioritization, and neutralization. This process ensures a coordinated and effective response to the multifaceted challenges posed by sophisticated cyber adversaries.

Effective Targeting

As Army Warrant Officers, 131As are well-versed in the Army's tactical targeting methodology known as D3A—Decide, Detect, Deliver, and Assess. Within USCYBERCOM, the JTC addresses targetable elements arising from strategic threats. Field Artillery Targeting Technicians are deeply integrated into the JTC process, from the strategic level down to the tactical level. This involvement includes Active Duty 131As and retired 131As who continue to serve as General Government employees or contractors.

The JTC is an iterative process that provides a flexible and adaptable framework for conducting targeting. In practice, phases of the JTC often occur concurrently, especially within tactical formations like the 780th MI Brigade (Cyber). This overlap typically arises from the need to synchronize efforts across multiple entities and frameworks to achieve mission objectives. For instance, a cyberspace capability may be developed before a targetable element is fully identified, or mission planning might proceed while a target is still being refined.

A 131A's expertise in the JTC allows their team to effectively utilize limited resources to achieve the Commander's desired end state.

So, what exactly are 131As doing to target threats similar to the previously mentioned one? We operationalize intelligence by guiding targets from their initial identification to final action. We transform Entities of Interest (EoI) into actionable, non-lethal reference points. 131As leverage their targeting expertise to layer effects, including those not directly controlled by the Commander, such as contributions from interagency and multinational partners. As Targeting Technicians, we continuously study joint publications and manuals to ensure the Joint Force Commander is fully informed about every aspect of a target and the cyberspace capabilities at their disposal. We are the driving force behind effects-based targeting. While every 131A metaphorically has a "crystal ball" at their desk to foresee the most suitable EoIs for nomination, this foresight is not infallible. We face unique challenges in conducting targeting within the cyber domain.

Figure 3. Field Artillery Logo

Endnotes

1. Microsoft Threat Intelligence (2024, July 3). Midnight blizzard: Guidance for responders on nation-state attack. Microsoft Security Blog.
2. Joint Publication 3-12 (2022, December 19) Joint Cyberspace Operations.
3. Joint Publication 3-60 (2018, September 28) Joint Targeting.
4. Job Qualification Record for the work role Fires Support Planner Master Level Version 2.0 as of July 2021 (2021, July)
5. United States Cyber Command National Mission Team Standardization (2020, October 28).
6. United States Cyber Command Combat Mission Team Standardization (2020, March 18).

The Army Cyberspace Capability Developer Technician Warrant Officer (170D): A Critical Enabler of Modern Warfare

By Chief Warrant Officer 3 Joshua Wellman, 170D, D Company, Operations Support Element

THE ARMY CYBERSPACE CAPABILITY DEVELOPER TECHNICIAN WARRANT OFFICER (170D) is a valuable member of the Army's Cyber Mission Force (CMF) responsible for developing and implementing critical software and hardware capabilities for cyberspace operations. As a Subject Matter Expert (SME) in cyber capabilities development, the 170D contributes to the Army's offensive and defensive missions. Our duties encompass analyzing system vulnerabilities, researching new technologies, documenting processes, providing expert guidance and mentorship, and supplying the operational force with the capabilities they need when they need them. However, as 170Ds, we can be more effective in this endeavor. Here are a few areas where we can focus on improvement:

Keep Your Toes in the Trenches

In today's fast-paced environment, individual developers often isolate themselves from customer interactions and requirements. Agile processes have section leadership serving as product owners, refining priorities based on customer feedback. While this approach works well when leaders have extensive experience, it's not always the case. As A 170D gains more development experience, they should regularly seek opportunities to engage with customers and operations.

Gene Kim captures this nicely in The Phoenix Project when he says: "Business agility is not just about raw speed… it's about how good you are at detecting and responding to changes in the market…" As a 170D, if you are missing from the table, how are you staying abreast of the operational environment?

A recent interaction with one of my senior leaders pointed out that we developed a capability based on a requirement, and that capability was never used in operations, raising questions about development priorities and the validity of the request. This statement reminded me of the genius of Dr. Ian Malcolm (Jurassic Park) when he said, "Your scientists were so preoccupied with whether or not they could, they didn't stop to think if they should." I'm not suggesting we say no to requested capabilities, but a better understanding of operational needs could have prevented waste or led to more effective solutions.

My rallying call here is to ensure 170Ds continue to keep a finger on the pulse of operations to guide the proper technical solution that meets the CMF's actual needs.

Learning is a Habit – Like Flossing, but Less Tedious

The Cyber landscape is constantly evolving, necessitating continuous learning for 170Ds. A combination of formal education and self-directed study, coupled with hands-on project experience, equips us with the knowledge and skills to remain at the forefront of our field. We certify at the Basic, Senior, and Master Job Qualification Record (JQR), just like the other MOSs. However, due to the wide range of senior specialties and the pace of technological changes, the 170D's education is never complete.

In Andrew Hunt and David Thomas's book called The Pragmatic Programmer, tip eight suggests: "Invest Regularly in Your Knowledge Portfolio." Just as you do in financial investing, the goal is to make this a habit, even in small amounts. They further elaborate that when you don't know something, be up-front. However, take it as a personal challenge to shore up the gaps in your knowledge. Be bold and ask questions, and don't be afraid to lean on one another. The Warrant Officer Cohort is stronger when we leverage the hive mind.

Risk-Averse is Just Code for 'Stuck in Neutral'

Leaving the confines of a Sensitive Compartmented Information Facility (SCIF) can be scary. I know the wash of rotating red lights can feel like a warm blanket. However, Captain James Tiberius Kirk said, "Risk… Risk is our business," and we can't let the good Captain down. As a 170D, you are more capable than you think, and a bit of diversity, within reason, can instill alternative perspectives that will allow you to mature as an officer and developer.

New Direction, Same Great Team

Emmerson said, "Do not go where the path may lead, go instead where there is no path and leave a trail." Cyber and technological innovations have clearly provided unique advantages on recent battlefields. The Army has seen the writing on the wall and is preparing for that next battle. I challenge all of us to imagine the role of a 170D and what we can bring to that fight. Stop obsessing about what has always been, ask hard questions, and think big ideas. After all, in the digital battlefield, the only thing more dangerous than a determined adversary is a Warrant Officer with a soldering iron and a sense of humor. ■

Experts in the undefined: Cyber Warfare Technicians and Offensive Cyberspace Operations

By Chief Warrant Officer 3 Justin Helphenstine, Technical Director, J3, U.S. Cyber Command

FOUR DOMAINS OF WARFARE TELL YOU, intuitively, what to expect from the military forces organized, trained & equipped to operate within them: land, sea, air, and space. The fifth domain diverges from this baseline: *Cyber* is a term with roots in the Greek κυβερνήτης;for 'helmsman', the same root whence the name 'Kubernetes'. A domain named after the act of navigation does not orient the beginner with the same immediacy as the 'land' domain or the 'sea' domain; cyber professionals therefore have no a *priori* heritage to explain their domain to outsiders. As Cyber Warfare Technicians, 170As stand in two domains: the richly understood land domain, with a domain-specific language lending itself to easy understanding, and an inchoate cyber domain which at first can appear bereft of the land domain's centuries of hard-won experience & wisdom. I say at *first* because this seeming challenge is a core to the value proposition of Cyber Warfare Technicians. 170As are uniquely situated as guides, able to lift the lamp of knowledge and illuminate a seemingly obscure domain.

This education role comes easier to some 170As than others. My defensive colleagues enjoy the benefit of rich investments by the private sector in charting the cyber domain and developing tools, training, and education to support the practitioner. The impact to shareholders of serious incidents incentivizes investment in characterizing cybersecurity in terms of hazards, probabilities, and mitigations – in other words, understanding the risks arising from reliance on the cyber domain. All of this investment offers a strong scaffolding for defensive cyberspace professionals. Further, the granting of master's degrees in cybersecurity would suggest a confidence among practitioners in the maturity of their profession.

The state of play is different in my own specialty. The phrase, "offensive cyberspace operations", deceptively simplifies our contribution to the Joint fight. My experience shapes my perspective that offensive-focused 170As are defined by a contradiction: we are subject matter experts for an inchoate domain; **expected to be masters of something the military has not yet mastered.** I think this contradiction creates tension for every offensive 170A, a tension made more evident as we progress from tactical toward strategic positions.

By inchoate, I do not believe movement and maneuver in cyberspace is undefined – computers are inherently intelligible systems. The knowledge of movement and maneuver between nodes in a network is well understood. Effects are also easy to understand, as anyone who has accidentally deleted important homework, or bricked a system such as to require a re-installation of the operating system, quickly grasps. Military operations employ tactics, but tactics are not the *ends*; they are not a strategy. Employment of the military instrument of national power implies a reason – a strategic purpose best accomplished by the military. From my vantage point, the class of problems best addressed with offensive cyberspace operations is incipient when set against the class of problems best addressed with a Joint Direct Attack Munition, a Freedom of Navigation transit, or an AIM-9 Sidewinder.

I mentioned earlier our cohort is uniquely situated to lift the lamp of knowledge. Against the incoherency of when best to apply offensive cyberspace operations, I see our role – and this is the role I play most often – as a guide to leaders seeking to convert our Nation's investments into effective tools of national power. As iron sharpens iron, so our charge is to help leaders understand the metes and bounds of cyberspace: what it is, what it is not, what can be done, and with what reliability. The latter two can be particularly difficult to explain: as discrete systems, computers are designed to process input; as complex systems they are capable of a wide range of unintended behavior. The answer to 'can you do X?' in cyberspace is frequently a qualified yes: the described sequence is likely *mechanically possible* but equally likely *highly improbable*, given myriad environmental factors across hosts and network segments. Even more unlikely is the ability to guarantee a particular sequence of actions with certainty at an arbitrary point in time – leading to unfavorable (for cyber) comparisons of the efficacy of a cyber effect contrasted with that of a JDAM. It takes more than technical acumen to educate leaders on the limiting factors of our domain even as we strive to find ways to accomplish the mission. I see this act of education, underpinned by an ability to translate cyberspace into the more intuitive language of maneuver, as the chief value proposition of 170As.

Cyber Warfare Technicians, particularly those focused on offensive cyberspace operations, occupy an exciting space. We sit at the forefront of the nation's developing sense of how best to employ cyberspace operations as an instrument of national power. This can lead to no small amount of frustration; I suspect I'm not the only one to ever feel like an unheeded Cassandra. But as professionals we must rise above that frustration. We must recognize the domain is still forming, the doctrine remains fungible, and that we do not have the luxury of constraining our thinking to well-understood problems and thoroughly rehearsed concepts. Our value proposition instead will lay in educating leaders, in helping those who develop policy and doctrine to sharpen their thinking. Leaders are entrusted with charting the course, but as with the Greek mariners of old, they will turn to the helmsman for navigation. With our origins as ships' masters in the Royal Navy, the domain may be new and loosely defined, but our role is ancient and fitting. ■

The Warrant Officer Identity

By Retired Chief Warrant Officer 3 Scott Brown, Brigade S-3 (operations) Current Operations, 780th Military Intelligence Brigade (Cyber)

WHEN CW5 JAMES RICHARDS, THE COMMAND CHIEF WARRANT OFFICER for the 780th MI Brigade (Cyber), approached me to write a BYTE article about the "Warrant Officer Identity" the first image that came to mind was a film that hit the big screen in 2002 titled "The Bourne Identity" with Matt Damon. It is an action movie about Jason Bourne, a CIA operative, who experienced amnesia while on a mission and throughout the storyline the audience watches as Jason Bourne gradually remembers details regarding his identity and unique occupation. It's an excellent movie and while the comparison between the main character and Warrant Officers requires some imagination, there are some obvious parallels worth pointing out. Both volunteered to undergo an extensive screening process to apply for acceptance into a program; both had to overcome physical and mental challenges to proceed through their initial training; and finally, both had to prove their ability to excel in uniquely challenging technical situations. If you haven't already, I recommend you watch the movie to better appreciate the comparison between Bourne and a Warrant Officer.

To gain a baseline appreciation of a Warrant Officer, let us review how the Army defines the personnel category per DA Pam 600-3 (Commissioned Officer Professional Development and Career Management) "The Army Warrant Officer is a self-aware and adaptive technical expert, combat leader, trainer, and advisor. Through progressive levels of expertise in assignments, training, and education, the Warrant Officer administers, manages, maintains, operates, and integrates Army systems and equipment across the full spectrum of Army operations. Warrant Officers are innovative integrators of emerging technologies, dynamic teachers, confident warfighters, and developers of specialized teams of Soldiers. They support a wide range of Army missions throughout their careers". While this description covers the broader roles of the Warrant community, I believe it accurately captures what an Army Warrant Officer is expected to do. Is it fair to say this is the Warrant Officer Identity?

While I'm sure there will be many different thoughts on this topic, I'm confident the Warrant Officer Identity is not revealed by what an individual does on a daily basis but through understanding why the individual has chosen this career path and observing how they meet the expectations of the Army and their unit. As an example, I believe a Warrant Officer thrives on being a professional and acknowledges that whether a person is serving in the military or employed in the commercial industry you don't become an adaptive technical expert, trainer, and advisor by working a traditional 40-hour work week. If excellence is truly achieved by practicing an act for 10,000 hours, a Warrant has the commitment to do just that. A Warrant Officer welcomes the challenge of integrating Army systems and equipment across the full spectrum of Army operations and takes pride in knowing the intimate details of a system down to the bolt, cable, and component. As a developer of specialized teams, a Warrant Officer understands and promotes the art of balancing mission success, Soldier development, and Family, because that delicate harmony maintains a ready and resilient force prepared to fight and win. The Warrant Officer performs these missions and more because that is the path they have willingly chosen. They know and accept their role as a subject matter expert and perform those responsibilities to the best of their ability. The soul of The Warrant Officer Identity is the why and how a task is completed, not what was actually achieved. If you join a Warrant Officer discussion to learn what happened, you will be disappointed. Often the topic will focus not on mission accolades, but technical talk describing what technique was utilized to correct a system fault or the creative tradecraft skills of a Team analyst. Warrant Officers know that successful mission accomplishment is required and through their unrelenting search for a refined and efficient process, confidently expect it.

There are numerous Warrant Officers in the Army supporting 47 specialties and 17 branches. All have navigated the challenges of completing Warrant Officer Candidate School (WOCS), most as a seasoned NCO. While this might not seem a difficult task, the sudden emersion in a Basic Training environment after years of permanent party service humbles the best of Soldiers. This training or rite of passage is the final part of the Warrant Officer Identity. This trial and the bond made with fellow Warrant Officers by completing WOCS seals your membership in the Warrant Officer Corps. When you look at a Warrant Officer head on, know there is a long line of active and retired Warrants standing behind ready to provide support when needed.

While "The Bourne Identity" was fictitious, The Warrant Officer Identity is real. I believe the article above accurately describes the fine men and women I served with in the Warrant Officer Corps, and I appreciate their continued support and mentorship to this day.

Advisor, Not Arcanist

By Chief Warrant Officer 2 Justin Melendez, Cyber Warfare Technician, 103 CMT, 782d Military Intelligence Battalion (Cyber)

I WANT TO BEGIN THE ARTICLE BY SAYING these writings reflect the perspective of a young CW2 170A (Cyber Branch) assigned to the 780th MI Brigade (Cyber). The opinions and examples present in this article by no means represent the entire Warrant Officer Cohort. The article is intended to be thought provoking and contrarian in nature. So, if this article triggers you in any way, good, that means we have something to talk about!

Contrary to popular belief, I disagree with the conventional phrasing that the Warrant Officer is the "technical expert, the subject matter expert, the end-all-be-all know it all". And maybe it's the fact that I am in the Cyber branch where I am surrounded by E-4, specialist 17C (Cyber Operations Specialists) digital natives who can run circles around me on a keyboard while chugging Mountain Dew and crushing Hot Cheetos.

Instead, when I see a Warrant Officer, I see someone who has a tenure of service. This tenure has enabled them to gain perspective based on learned skills, experience, and relationships. This Warrant Officer can break through barriers of bureaucracy, conventional wisdom, and personalities to find a commander the optimal solution. The Warrant Officer is highly conscious of their surroundings and resources, utilizing their experience to effectively employ these capabilities in real-time to fulfill the commander's intent. I feel that the days of the haggard "chief" being the encyclopedia Britannica of the team room are largely over.

Imagine a time where the Army had a direct commissioning program where they could *"provide an opportunity for professionals with cyber-related education and/or experience to be directly appointed into the Army's Cyber Corps in the ranks of lieutenant through colonel"* (Army Cyber Direct Commissioning Program - U.S. Army Cyber Command). Now imagine there's a captain, a captain with a PhD in data science, he's highly skilled and trained in cutting-edge technology but lacks awareness of the bureaucracy that is looking to eat his ideas for lunch. His talents seem wasted amidst constant distractions of the status quo, his duties as a junior officer, and non-negotiable key developmental milestones. How do we make sure his talents and opinions aren't falling on deaf ears? In steps the Warrant Officer as the advocate for his valuable insights. The Warrant Officer is technically fluent enough to recognize the value in his disruption. The Warrant Officer is also able to separate the wheat from the chaff…he knows who to talk to and most importantly who not to talk to. He knows what questions to ask, and he knows when it's appropriate to not just take no for an answer. And ultimately the Chief can build the bridge between good idea and practical employment. The Warrant Officer's experience and credibility has created an environment for the young officer to win, an environment where the Army benefits from an asset well utilized.

Now the example above is a fable but is not far from reality. This captain really exists, he just wasn't a product of the Army's cyber direct commissioning program. Luckily, he is a result of the Army's organic recruiting efforts. However, there seems to be a concerted effort to attract and acquire more talent of this form. My question to you is are we ready to manage this talent? What role do we as Warrant Officer's play in this initiative?

As a branch, we should embrace the fact that we have extremely intelligent, motivated, and well-educated junior enlisted and officers that can prove to be more technically capable than us. We should reconsider our interpretation of the moniker "technical-expert". We should re-shape our identity from one of the village elder to one who enables those around us to accomplish the mission. We should leverage our tenure to their benefit. We should enable them to leverage our voice and credibility. When I look in the mirror, I see a connector, I see an enabler, I see an asset to the commander, I don't see a wizard. ■

The Multi-Faceted Professional

By Warrant Officer Axel O. Nieves, Cyber Warfare Technician, Detachment-Texas, 782d Military Intelligence Battalion (Cyber)

IN THE REALM OF MILITARY LEADERS, THE ROLE OF THE WARRANT OFFICER is pivotal. My identity as a Warrant Officer is shaped by intelligence, adaptability, and a continuous quest for learning. My journey as a warrant officer underscores an unwavering commitment to excellence, driven by a deep understanding that leaders evolve with both environmental demands and personal growth.

Intelligence: The Cornerstone of Expertise

The cornerstone of my role as a Warrant Officer is intelligence. This extends beyond normal cognitive abilities, I personally do not have the best memory, and I am certainly not the smartest in my unit on everything, but intelligence involves more than just acquiring knowledge. It involves the ability to apply it in real-life scenarios. My position demands a keen grasp of complex systems and the skill to make informed and practical decisions under pressure.

The modern cyber landscape, marked by rapid technological advancements and evolving threats, requires me to stay current and adapt. Mastering new technologies and anticipating future challenges are essential. My intelligence enables me to integrate diverse elements into coherent strategies, ensuring our operations remain effective and agile.

Flexibility: Adapting to a Dynamic Environment

Flexibility is another defining characteristic of my role as a Warrant Officer. The military is dynamic, with no two years alike, making adaptability crucial. The ability to pivot in response to shifting priorities, unforeseen obstacles, or evolving mission parameters is vital. My flexibility allows me to navigate these changes seamlessly, ensuring effectiveness regardless of circumstances.

Being flexible means embracing change rather than resisting it. This involves quickly assimilating new information, adjusting strategies on the fly, and maintaining a positive outlook even in challenging situations. Rigid adherence to pre-established plans can hinder progress, while a flexible approach fosters innovation and resilience. This adaptability enhances my performance and sets a standard for my peers, promoting a culture of agility and responsiveness.

Openness to Challenges and New Learning Experiences

Openness to challenges and new learning experiences is a critical aspect of my role. Embracing difficulties head-on and seizing opportunities for growth is essential for both personal and professional development. In the ever-evolving military landscape, complacency is detrimental, while curiosity and a readiness to learn drive progress and excellence.

Throughout my 17-year career, I've sought challenges that push me beyond my comfort zone. This proactive approach has allowed me to acquire new skills, gain diverse experiences, and expand my understanding of military operations. Welcoming new learning experiences ensures I remain at the forefront of my field, capable of addressing emerging issues with innovative solutions.

This openness extends to collaboration and learning from others. The military is a team sport, and exchanging ideas with my fellow teammates is invaluable. Each interaction is approached with a mindset of mutual learning, recognizing that everyone has unique insights to offer. This collaborative spirit enhances my capabilities and contributes to our team's overall effectiveness.

Integrating Intelligence, Flexibility, and Openness

The synergy between intelligence, flexibility, and openness defines my role as a multifaceted Warrant Officer. These attributes interact and reinforce each other, creating a dynamic and effective approach to leadership and problem-solving. Intelligence provides the foundation upon which flexibility and openness are built, enabling me to navigate complexities with insight and adaptability.

For example, when facing a new technological challenge, my intelligence helps me understand the core principles and potential impacts. Flexibility allows me to adapt to changing requirements, while openness drives me to explore innovative solutions. This holistic approach ensures I am prepared to address current demands and anticipate future challenges.

In conclusion, being a multifaceted warrant officer reflects my commitment to excellence through intelligence, flexibility, and openness to new experiences. These qualities define my leadership approach, enabling effective contributions to mission success and inspiring those around me. ■

Cyber's Swiss Army Knives: Warrant Officers

By Warrant Officer Roy D. Cracraft, Exploitation Analyst, C Company, 782d Military Intelligence Battalion (Cyber)

AS A CYBER WARRANT OFFICER, I embody a unique blend of technical expertise, leadership, strategic insight, ethical commitment, and adaptability. My role is defined by a deep understanding of cybersecurity principles and technologies, complemented by a continuous pursuit of knowledge to stay ahead of emerging threats. I serve as a crucial leader and mentor, bridging the gap between enlisted personnel and command, while translating complex technical issues into actionable strategies. Strategic thinking enables me to anticipate and address potential vulnerabilities, ensuring efficacy and security. Upholding strict technical, ethical, and legal standards is essential in managing sensitive capabilities, and my adaptability ensures effective responses to the dynamic nature of cyber threats. Together, these attributes define my role and underscore my contribution to maintaining robust cyber operations and security.

In military operations, the role of a Cyber Warrant Officer has become increasingly pivotal. As a Cyber Warrant Officer, my role is defined by a unique combination of technical proficiency, leadership capabilities, and an unwavering commitment to securing and managing cyber operations. What makes me a Cyber Warrant Officer is not just the skills I possess, but the mindset and ethos that drive my approach to this critical role.

Firstly, my identity as a Cyber Warrant Officer is anchored in a deep and comprehensive understanding of cybersecurity principles and technologies. Unlike other positions within the military, my role demands a specialized knowledge of networks, information systems, and cyber threats. This knowledge is not static but evolves continuously with advancements in technology and changes in the cyber threat landscape. My ability to stay up to date with these developments is crucial. I engage in continuous learning and collaboration with industry experts to ensure my skills remain cutting-edge. This commitment to knowledge is a fundamental aspect of what defines me as a Cyber Warrant Officer.

In addition to technical expertise, what sets me apart is my role as a leader and advisor within the cyber domain. As a warrant officer, I serve as a bridge between the enlisted personnel and the command structure. This role requires not only technical skills but also the ability to mentor and guide junior personnel. My leadership is characterized by a focus on developing others, fostering a collaborative environment, and ensuring that all team members are equipped with the necessary skills and knowledge to accomplish the mission. Effective communication is central to my leadership style. I must translate complex technical issues into actionable strategies for senior officers and clear instructions for my team. My ability to navigate these different communication demands is crucial in maintaining the efficiency and effectiveness of our cyber operations.

Furthermore, my role involves strategic thinking and decision-making. Cyber operations are not just about reacting to immediate threats or actioning a target, but also about anticipating potential vulnerabilities and preparing for future challenges. This strategic perspective requires a balance of analytical skills and creativity. I must assess risks, develop mitigation strategies, and implement solutions that align with broader military objectives. This strategic mindset allows me to anticipate and counteract cyber threats proactively, ensuring the greatest chances of success, as well as resilience and security of our cyber infrastructure.

Another defining aspect of my role is the ethical and legal responsibilities of managing sensitive information and cyber operations. As a Cyber Warrant Officer, I am entrusted with access to classified and confidential data. I must adhere to strict ethical standards and legal guidelines in handling this information. My commitment to integrity and accountability ensures that all operations are conducted within the bounds of the law and military regulations. Upholding these standards is essential in maintaining trust and credibility within the military and with our partners.

Lastly, adaptability and resilience are core attributes that define me as a Cyber Warrant Officer. The nature of cyber threats is dynamic and unpredictable, often requiring quick thinking and the ability to adapt to rapidly changing situations. Whether it's responding to a new cyber-attack or integrating emerging technologies, my ability to remain flexible and resilient is crucial. This adaptability ensures that I can effectively address evolving challenges and support our mission in an ever-changing cyber landscape.

In conclusion, what makes me a Cyber Warrant Officer is a blend of specialized technical knowledge, leadership and mentorship capabilities, strategic thinking, ethical integrity, and adaptability. These attributes collectively define my role and enable me to contribute effectively to the mission of safeguarding our cyber domain. As cyber threats continue to evolve, the importance of my role and the qualities that define me will remain integral to maintaining our security and operational success. ■

Warrant Officer Candidate

By SSG Dereck J. Cottrille, Headquarters and Headquarters Company, 780th Military Intelligence Brigade (Cyber)

I AM STAFF SERGEANT COTTRILLE. I have been in the Army nine years as a 35N and currently serve as the BDE S3 TREX (Training and Exercise) NCOIC. As a Warrant Officer Candidate, I am on the cusp of fulfilling a goal I have chased since my first duty station and became engulfed with everything SIGINT (Signals Intelligence). Heading into Warrant Officer Candidate School, I am anxious but also excited on how my career will unfold as a Warrant Officer. The NCO in me is excited for the challenge to not only continue training enlisted Soldiers and NCOs but also take on the task of being an advisor to my future commanders.

I view the Warrant Officer role as being the subject matter expert in their tradecraft and using that knowledge to help and guide junior Soldiers, NCOs, and commissioned officers alike to complete the mission from a tradecraft specific perspective. What separates me from being an NCO and being a SIGINT Warrant is the ability to dive headfirst into the SIGINT realm. At this stage of my NCO career, I have moved into a more administrative role with managing staff tasks and Soldiers at the staff level instead of being at the operational level of SIGINT within a Team or Squad. As a SIGINT Warrant, I can shift my focus to lead and advise both operationally and administratively through the entirety of the SIGINT production chain.

A piece of advice I would like to leave aspiring Warrant Officers is to not apply due to not being “ready” or “well-rounded.” I spent several years thinking that I need certain amount of tactical and strategic time to be a “well-rounded” SIGINT Warrant. I think this is a misconception we have heard or expected of ourselves as junior Soldiers or NCOs when finding our way through the Army. I spent most of my career in tactical units and have been in a staff position since coming to the 780th MI Brigade. The number one thing I learned during that time is that I learned through personal experience of how to be a SIGINT NCO so how would I learn to be a SIGINT Warrant if I didn’t become one. Through the application process and advice from senior Warrant Officers, I learned that if you are looking for “well-rounded” you should look at the variety of skills that make you the best version of yourself. Then look at how you tie those into your given MOS to adapt, improve those within your sphere of influence and organization, and ultimately succeed in the tasks or circumstances that stand before you. ■

En Garde

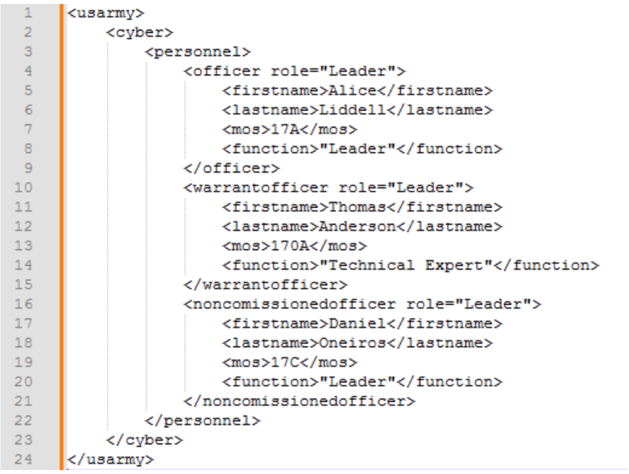
By Chief Warrant Officer 3 Jason Ehlinger, Cyber Operations Technician, 781st Military Intelligence Battalion (Cyber)

Anyone who witnesses an assembly of Warrant Officers usually experiences a level of shock and awe at so many elusive personnel being present under direct observation. Unbeknownst to these witnesses, these assemblies are rare because they induce a specific risk.

The Army calls the Warrant Officers a Cohort. The Warrants prefer to call themselves a Wolf Pack in local circles. However, a physical collection of Warrants follows the Law of Large Numbers. The greater the number of Warrant Officers present, the more likely a specific conversation topic will come up. Here, we leave the safety of math for the danger of particle physics. Here, we achieve a Criticality.

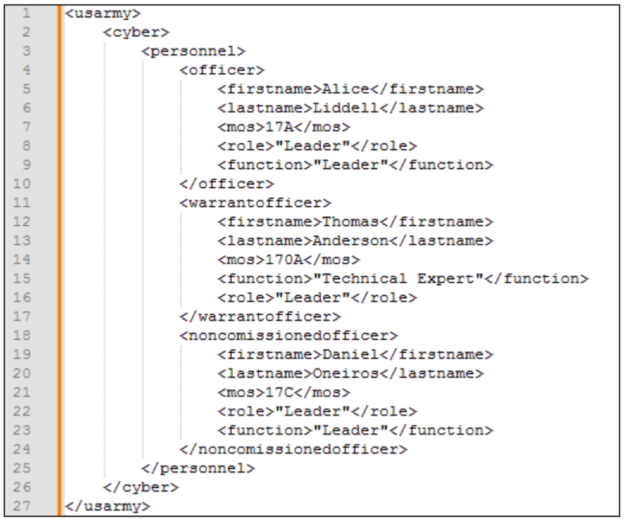
In this super state, Warrant Officers must discuss the merits of Old Guard versus New Guard, where their opinion is on that spectrum, and provide points and counterpoints for each other's points and counterpoints based on their viewpoint. No one is wrong, no one is right, and as these chain reactions go in physics, the conversation is wont to go indefinitely.

The debate is essentially the following:



```
<usarmy>
    <cyber>
        <personnel>
            <officer role="Leader">
                <firstname>Alice</firstname>
                <lastname>Liddell</lastname>
                <mos>17A</mos>
                <function>"Leader"</function>
            </officer>
            <warrantofficer role="Leader">
                <firstname>Thomas</firstname>
                <lastname>Anderson</lastname>
                <mos>170A</mos>
                <function>"Technical Expert"</function>
            </warrantofficer>
            <noncomissionedofficer role="Leader">
                <firstname>Daniel</firstname>
                <lastname>Oneiros</lastname>
                <mos>17C</mos>
                <function>"Leader"</function>
            </noncomissionedofficer>
        </personnel>
    </cyber>
</usarmy>
```

Figure 1. New Guard.

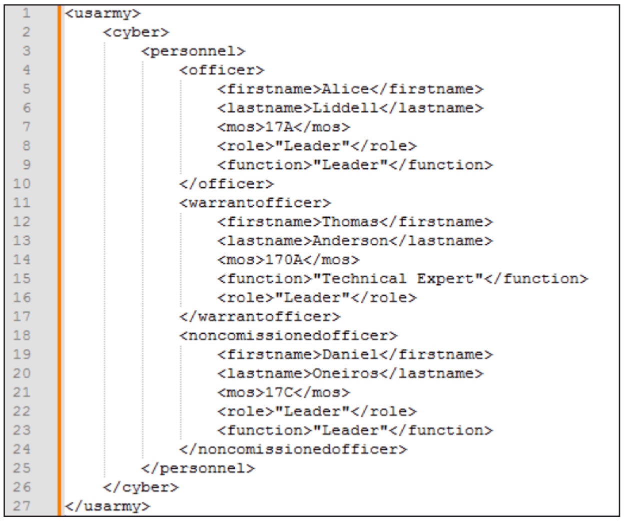


```
<usarmy>
    <cyber>
        <personnel>
            <officer>
                <firstname>Alice</firstname>
                <lastname>Liddell</lastname>
                <mos>17A</mos>
                <role>"Leader"</role>
                <function>"Leader"</function>
            </officer>
            <warrantofficer>
                <firstname>Thomas</firstname>
                <lastname>Anderson</lastname>
                <mos>170A</mos>
                <function>"Technical Expert"</function>
                <role>"Leader"</role>
            </warrantofficer>
            <noncomissionedofficer>
                <firstname>Daniel</firstname>
                <lastname>Oneiros</lastname>
                <mos>17C</mos>
                <role>"Leader"</role>
                <function>"Leader"</function>
            </noncomissionedofficer>
        </personnel>
    </cyber>
</usarmy>
```

Figure 2. Old Guard.

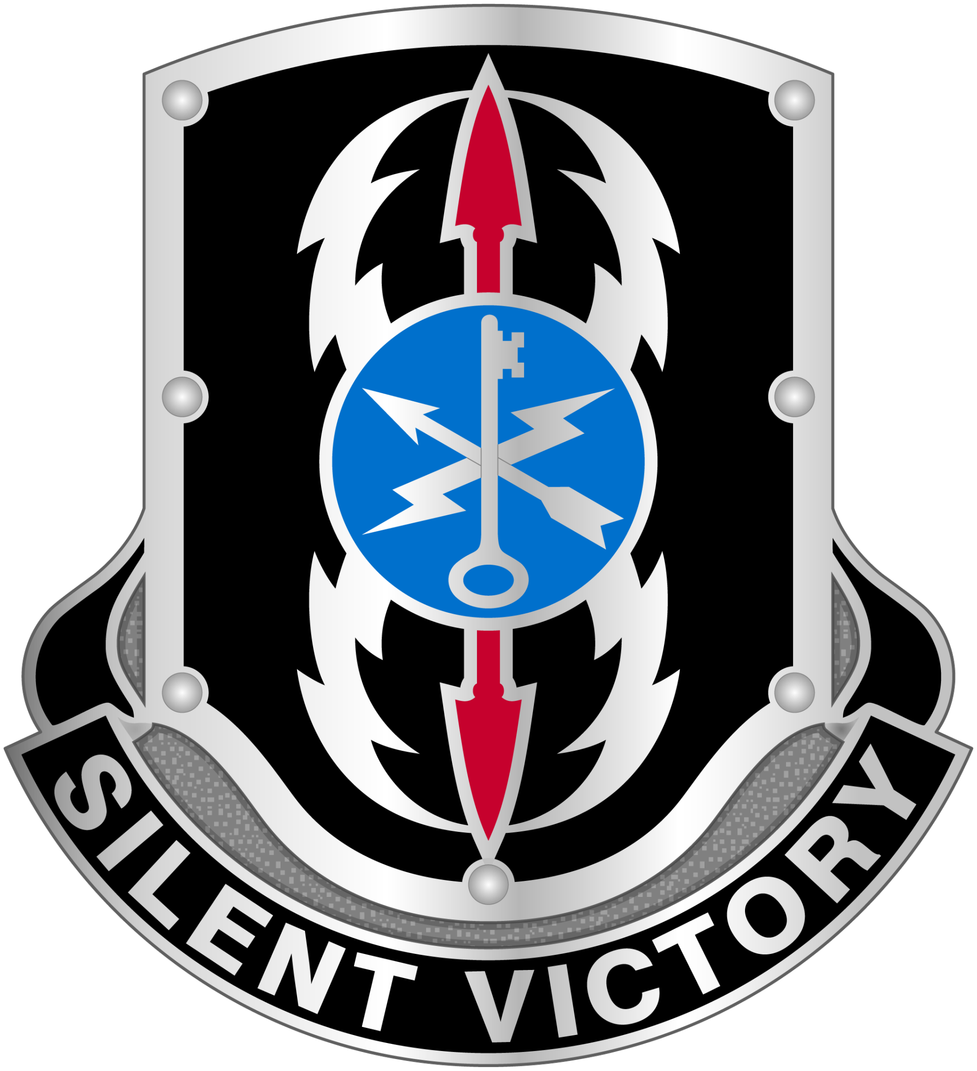
Certainly, an engaging topic, but a conversation I almost never participate in. My opinion on the matter is dangerous. Expressing my opinion to a Criticality of Warrants has a high risk of causing the assemblage to go Super Critical.

My opinion is:



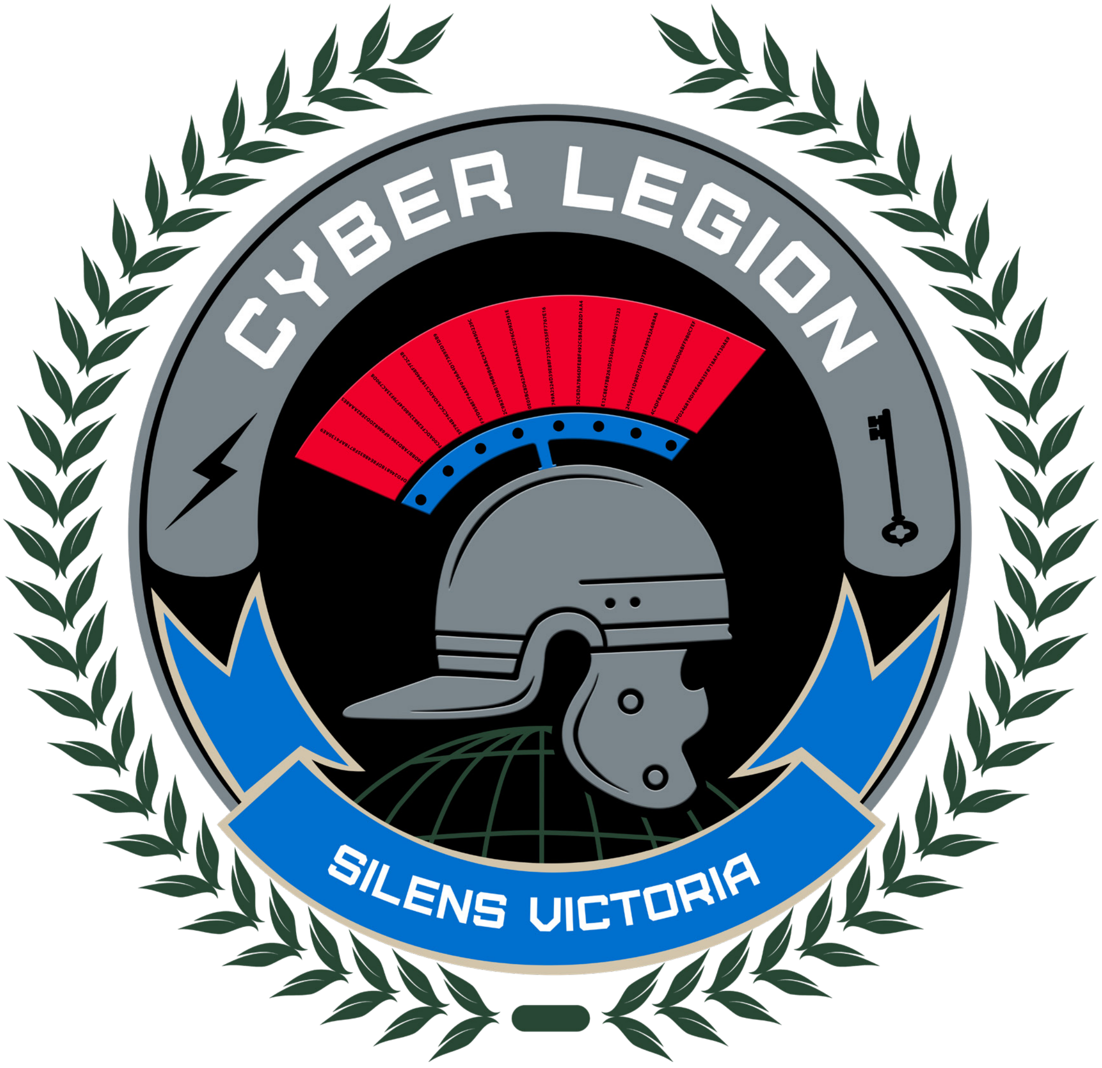
```
<usarmy>
    <cyber>
        <personnel>
            <officer>
                <firstname>Alice</firstname>
                <lastname>Liddell</lastname>
                <mos>17A</mos>
                <role>"Leader"</role>
                <function>"Leader"</function>
            </officer>
            <warrantofficer>
                <firstname>Thomas</firstname>
                <lastname>Anderson</lastname>
                <mos>170A</mos>
                <function>"Technical Expert"</function>
                <role>"Leader"</role>
            </warrantofficer>
            <noncomissionedofficer>
                <firstname>Daniel</firstname>
                <lastname>Oneiros</lastname>
                <mos>17C</mos>
                <role>"Leader"</role>
                <function>"Leader"</function>
            </noncomissionedofficer>
        </personnel>
    </cyber>
</usarmy>
```

782nd Military Intelligence Battalion (Cyber) DUI Symbolism:



Symbolism. Oriental Blue and Silver Gray are the traditional colors associated with the Military Intelligence Corps. The shape of the shield recalls that of Roman legionaries and conveys the chosen nickname of the battalion, "Cyber Legion." The arching lightning bolts are associated with electromagnetic and cyberspace operations, signifying the mission of the battalion. The spears denote offensive maneuvers and are colored red to indicate victories in "Red Space," the portions of cyberspace controlled by adversaries. The blue disc conveys the unit's worldwide scope and global power projection. The arrow indicates readiness, the lightning bolt implies cyber warfare, and the key suggests secrecy and alludes to the battalion's motto, "Silent Victory." The seven rivets on the border, the figure-eight shape of the arched lightning bolts, and the two spearheads stand for the numerical designation of the battalion, 782d.

Logo Symbolism:



Symbolism. The prominent Roman helmet represents the battalion's primary weapon system – the Cyber Legionary. It is oriented as if worn in combat, charging forward into battle. The plume is red, symbolizing the adversary "red space" where cyber legionaries operate. The Soldier's Creed is cryptographically hashed in the plume, never forgotten by Cyber Legionaries even when operating in enemy networks.

The globe represents global power projection. It is Army Green as Army teams are the best of U.S. Cyber Command's Combat Mission and Support Teams.

The two banners represent the vast majority of the battalion's personnel. The top banner is Cyber *Steel Grey* while the bottom banner is Military Intelligence *Oriental Blue*. Embedded in the top banner is the heritage of signals intelligence, electromagnetic warfare, and secrecy as represented by the lightning bolt and key. Our name, "Cyber Legion," is the top banner and our Latin motto, "Silens Victoria" meaning "Silent Victory," is in the bottom banner. The laurels in Army green signify victory.

Task Force Echo Color Casing Ceremony Signifies the End of a Historic Mission

By Steven Stover, Public Affairs Officer, 780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, MD. – Col. Candy Boparai, commander of the 780th Military Intelligence (MI) Brigade (Cyber), hosted a Casing of the Colors ceremony for Task Force Echo, marking the end of the TFE mission, at the Captain John E. Smathers United States Army Reserve Center, August 6.

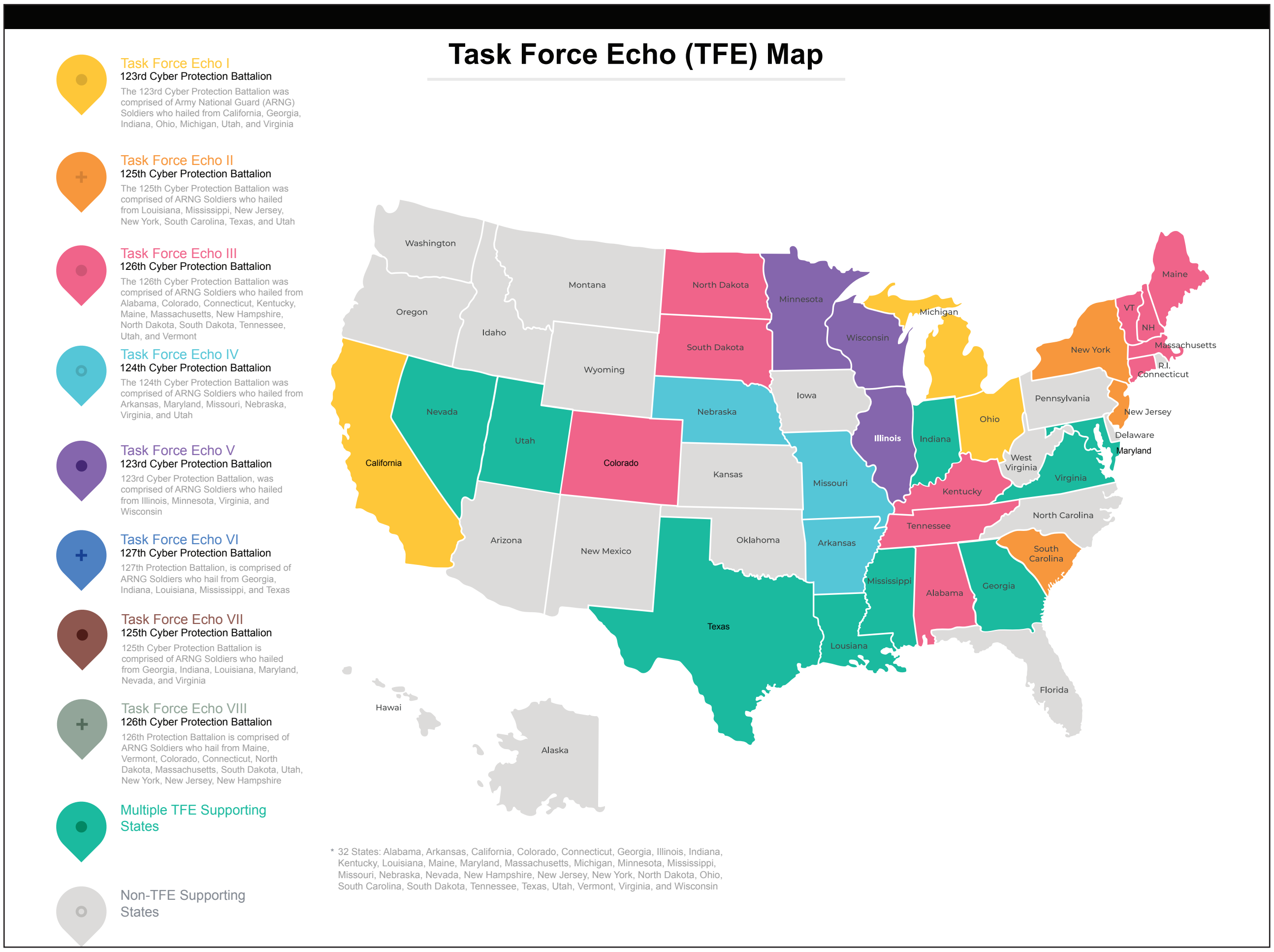
The official party for this historic event included Boparai; Command Sgt. Maj. Joseph P. Daniel, the senior enlisted leader of the 780th MI Brigade (Cyber); Col. Russel E. McGuire, commander of the 91st Cyber Brigade, Virginia Army National Guard (VA ARNG); and Command Sgt. Maj. Michael S. Rivera-Wenger, the senior enlisted leader of the 91st Cyber Brigade.

Since inception, TFE has been aligned under, and operationally controlled by the 780th MI Brigade (Cyber) and administratively controlled by U.S. Army Cyber Command (ARCYBER).

The casing of the colors is significant in that it symbolizes the final chapter in TFE history and signifies the end of the TFE mission and the release of TFE VIII from its present assignment with ARCYBER and its reassignment to the 91st Cyber Brigade, VA ARNG.

The final TFE VIII rotation was commanded by Lt. Col. Karmin Ng, commander of the 126th CPB, and the senior enlisted leader is Command Sgt. Maj. Daniel P. Doherty. The 126th CPB was activated on November 5, 2017, at Camp Edwards, Massachusetts, and previously mobilized on the third rotation of TFE on March 13, 2019.

"Into the Darkness, We Bring the Light"
"Everywhere and Always…In the Fight!" ■



Task Force Echo (TFE) Map

Task Force Echo I
123rd Cyber Protection Battalion
The 123rd Cyber Protection Battalion was comprised of Army National Guard (ARNG) Soldiers who hailed from California, Georgia, Indiana, Ohio, Michigan, Utah, and Virginia

Task Force Echo II
125th Cyber Protection Battalion
The 125th Cyber Protection Battalion was comprised of ARNG Soldiers who hailed from Louisiana, Mississippi, New Jersey, New York, South Carolina, Texas, and Utah

Task Force Echo III
126th Cyber Protection Battalion
The 126th Cyber Protection Battalion was comprised of ARNG Soldiers who hailed from Alabama, Colorado, Connecticut, Kentucky, Maine, Massachusetts, New Hampshire, North Dakota, South Dakota, Tennessee, Utah, and Vermont

Task Force Echo IV
124th Cyber Protection Battalion
The 124th Cyber Protection Battalion was comprised of ARNG Soldiers who hailed from Arkansas, Maryland, Missouri, Nebraska, Virginia, and Utah

Task Force Echo V
123rd Cyber Protection Battalion
123rd Cyber Protection Battalion, was comprised of ARNG Soldiers who hailed from Illinois, Minnesota, Virginia, and Wisconsin

Task Force Echo VI
127th Cyber Protection Battalion
127th Protection Battalion, is comprised of ARNG Soldiers who hail from Georgia, Indiana, Louisiana, Mississippi, and Texas

Task Force Echo VII
125th Cyber Protection Battalion
125th Cyber Protection Battalion is comprised of ARNG Soldiers who hailed from Georgia, Indiana, Louisiana, Maryland, Nevada, and Virginia

Task Force Echo VIII
126th Cyber Protection Battalion
126th Protection Battalion is comprised of ARNG Soldiers who hail from Maine, Vermont, Colorado, Connecticut, North Dakota, Massachusetts, South Dakota, Utah, New York, New Jersey, New Hampshire

Multiple TFE Supporting States

Non-TFE Supporting States

* 32 States: Alabama, Arkansas, California, Colorado, Connecticut, Georgia, Illinois, Indiana, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, and Wisconsin

Praetorian Soldiers and Civilians answer the call to overcome recruiting and retention challenges

By Steven P. Stover, Public Affairs Officer, 780th Military Intelligence Brigade (Cyber)

FORT GEORGE G. MEADE, MD. – Praetorian Soldiers and Civilians with the 780th Military Intelligence Brigade (Cyber) continue to network with the American people locally and throughout the United States to educate and inform thousands of Americans on the life-changing opportunities of Army service as a cyberspace operator, developer, intelligence analyst, or linguist.

Working in partnership with our garrison public affairs offices the brigade has built partnerships with area schools and libraries to send out ambassadors to tell their Army story, host computer challenges, and provide classes on various STEM (science, technology, engineering and mathematics) workshops.

"We are very proud of the work our Soldiers and Civilians do to tell our Army story to our community and the American people more broadly," said Col. Candy Boparai, commander of the 780th MI Brigade (Cyber). "I think that the 780th MI Brigade (Cyber) has a unique story to share, and if sharing that story can inspire more Americans to consider service specifically in the U.S. Army, or the Department of Defense more generally, then we are very glad to have the opportunity to do just that."

This fall the brigade will host Hackathon IV in partnership with the Anne Arundel County Public Library, to encourage teen interest in STEM. The fourth annual fall event will include a Capture the Flag (CTF) competition, Logic Games, OSINT (open-source intelligence – what Personal Identifiable Information (PII) can be easily found on social media) and Python Development stations, and will take place from 4 to 7 p.m., September 10, October 8 and November 19, at the Odenton Regional Library, AACPL, Odenton, Maryland. Visit the Anne Arundel County Public Library page to register at https://www.aacpl.net/event/hackathon-162093.

"I firmly believe we all have people in our past that enabled us to get to where we are. Therefore, we each have a responsibility to take what we have learned and pass that on to someone else," said Chief Warrant Officer 3 Joshua Wellman, a cyber capabilities developer technician (170D) assigned to the Operations Support Element (OSE), 780th MI Brigade (Cyber), and the lead developer for the CTF – cyber challenge. "Outreach events like this are one way in which we can do this. They also have the advantage that the skills learned could one day be used to defend our nation. Also, they're just outright fun!"

Additionally, Praetorian Soldiers and Civilians partner with U.S. Army Cyber (ARCYBER) Talent Management (TM); U.S. Army Recruiting Command; the Illinois Institute of Technology, a National Center of Academic Excellence in Cyber Defense Education; and Maryland STEM Festival, to support the Total Army Involvement in Recruiting (TAIR) and the U.S. Army Intelligence and Security Command (INSCOM) Vigilance Recruiting programs.

In 2024, the brigade provided TAIR support for 13 high school events at Paul M. Dorman High School, Roebuck, S.C.; Blythewood High School, Blythewood, S.C.; Greenwood High School, Greenwood, S.C.; Hephzibah Comprehensive High School, Hephzibah, Ga.; TC Roberson High School, Asheville, N.C.; schools throughout Clark County School District in Greater Las Vegas; Northern Illinois University; Rock Falls High School, Rock Falls, Ill.; Rockford East High School and Guilford High School in Rockford, Ill.; Hononegah Community High School, Rockton, Ill.; Moon Area High School, Moon Township, Pa.; and the George Westinghouse High School in Brooklyn, N.Y., as well as outreach support to ChiCyberCon, hosted by Illinois Tech in Chicago; a Total Army Recruitment and Outreach Event in Arlington, Texas; and the AI Expo for National Competitiveness, in the Washington DC Convention Center.

The Praetorians will next send a team to support ARCYBER TM in the 2nd Total Army Recruitment and Outreach Event at NRG Stadium in Houston, Texas, September 6 and 7.

The 780th MI Brigade (Cyber) is filled with talented and professional individuals.

Sgt. 1st Class Gerardo Martinez, a 35N, signals intelligence analyst, built three computer challenges for the Moon Area High School students including steganography, port scanning, and the most popular of all, password cracking. Additionally, Spc. Garrett Kemp, a 17C, cyber operations specialist, ran a global threat map, using a mobile hotspot that displayed all the worldwide cyberattacks, which was an excellent way to move students into the laptop containing the challenges.

Capt. Ryan Johnson, a 17A, cyberspace operations officer, and Spc. Shelby Seale, a 17C, provided TAIR support to five high schools for the U.S. Army Columbia Recruiting Battalion, USAREC, by building a small demonstration in which the Soldiers or students would run through a simple example of exploiting a Windows Server using Kali Linux and Metasploit and they would reboot the target system. Throughout the five-day trip the soldiers gave the demonstration and overview to several thousand students.

Robert Ighnat, an OSE Interactive

On-net Operator (ION), represented the brigade, the Army Civilian Corps, and the U.S. Army, on two ChiCyberCon panels: the "Understanding Cybersecurity Fundamentals" and "Building a Career in Cybersecurity" breakout sessions.

Although not U.S. Army recruiters, the Soldiers and Civilians engage with interested students and young professionals – many unaware of cyber as a profession in the Army – about their work roles, day-to-day activities, necessary certifications and technical qualifications – many of which can be provided by the Army's Cyber Center of Excellence at Fort Eisenhower, Ga. – and discuss brigade Civilian employment opportunities.

In addition to opportunities to travel and engage the American people, the brigade has fielded a competitive Army Ten-Miler (ATM) team, a competitive cyber team, and a Bataan Memorial Death March team in 2024. 1st Lt. Kristen Gray, from Park Ridge, N.J., is a 17A, cyberspace operations officer, a member of the Howard County Striders Racing Team, and she placed 3rd in the military female category of the 39th Army Ten-Miler race, October 8, 2023. The brigade will host time trials on August 7 for the 40th ATM Praetorian team.

And did you know the Praetorians host an annual AvengerCon? AvengerCon is 780th MI Brigade's homegrown hacker conference – run by Soldiers and Civilians for Army Soldiers and Civilians, as well as other Department of Defense and Intelligence Community partners, Veterans, academia, and students.

"AvengerCon is a computer security conference hosted by members of the 780th Military Intelligence Brigade," said Capt. Jake Heybey, a 17A, 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."

AvengerCon IX is scheduled for February 26 and 27, 2025 at the Georgia Cyber Innovation & Training Center.

"We need to reach a new generation of Americans and share with them the life-changing opportunities that come with service in the U.S. Army…and we need all of you to help us tell the Army story and inspire more Americans to serve," said Secretary of the Army Christine E. Wormuth.

The Soldiers and Civilians of the 780th MI Brigade (Cyber) are certainly doing their part to tell their Army story and inspiring more Americans to serve.

"Everywhere and Always…in the Fight!"
#ArmyPossibilities #BeAllYouCanBe

Praetorians "Everywhere and Always…In the Fight!" Change of Command

FORT GEORGE G. MEADE, Md. *– Maj. Gen. Timothy D. Brown, commanding general, United States Army Intelligence and Security Command, hosted a change of command ceremony whereby Col. Benjamin F. Sangster relinquished his command of the 780th Military Intelligence Brigade (Cyber), Praetorians, to Col. Candy Boparai in a ceremony on McGlachlin Parade Field, June 21.*

In a ceremony steeped in Army tradition, the Soldiers representing the Headquarters and Headquarters Company (Hastati); 781st Military Intelligence (MI) Battalion (Vanguard); 782nd MI Battalion (Cyber Legion); 11th Cyber Battalion (Leviathans); Operations Support Element; and Task Force Echo, 126th Cyber Protection Battalion, Army National Guard; stood in formation to bid farewell to their departing commander and to welcome a new one.

Vanguard…When Others Cannot, Change of Command Ceremony

FORT GEORGE G. MEADE, Md. *– The 781st Military Intelligence Battalion (Cyber) change of command whereby Lieutenant Colonel Donald E. Sedivy relinquished his command to Lieutenant Colonel Scott A. Beal in a ceremony hosted by Colonel Benjamin F. Sangster, commander of the 780th Military Intelligence Brigade (Cyber), on the McGlachlin Parade Field, June 17. Vanguard "When Others Cannot"*

C Company (Capybara), 11th Cyber Battalion Activation Ceremony

Momentous activation of Army unit to meet the threats and challenges of the future battlefield

***FORT EISENHOWER, Ga.** – Lt. Col. Luis Etienne, commander of the 11th Cyber Battalion (Leviathans), 780th Military Intelligence Brigade (Cyber), hosted an activation ceremony for "Charles" Company (Capybara), 11th CY, and introduced the new Capybara command team, Capt. Sean Cushman and 1st Sgt. Terry Spangler at the Eisenhower Conference Center, July 11.*

781 MI BN (Cyber) Organization Day

THE NORTH FACE
Loyalty

Vanguard Battalion Commander’s Cup 2024

FORT GEORGE G. MEADE, Md. – LTC Scott Beal, commander, 781st Military Intelligence Battalion (Cyber), and CSM Jermaine Ocean, the battalion's senior enlisted leader, hosted the Vanguard Commander's Cup this week, culminating in an Organization Day at Burba Lake Pavilion Three, August 15.

By day's end, there can only be one… B Company, Bravo Immortals, 781st MI Battalion took home the Vanguard Commander's Cup for 2024. Vanguard… When Others Cannot.

782 MI BN (Cyber) Organization Day

SILENT VICTORY

Cyber Legion Commander's Cup and Organization Day

FORT EISENHOWER, Ga. – *The 782d Military Intelligence Battalion (Cyber) hosted their 2024 Commander's Cup sports events the past two weeks, including a basketball, flag football, kickball, soccer, and volleyball competition, culminating in a battalion organization day on Friday, June 14. "Cyber Legion…Silent Victory" (Army Photos by SSG Torin Marion)*

782 MI BN (Cyber)
INSCOM PT

INSCOM command team conducts physical training with Cyber Legion

__FORT EISENHOWER, Ga.__ – Maj. Gen. Timothy Brown, commanding general, U.S. Army Intelligence and Security Command (INSCOM), and Command Sgt. Maj. Kyle Gillam, the INSDCOM senior enlisted leader, conduct physical training with Soldiers of the 782nd Military Intelligence Battalion (Cyber Legion), 780th MI Brigade (Cyber), July 19. "Vigilance Always" "Everywhere and Always…In the Fights!" (Army Photos by SSG Torin Marion)

11th Cyber Battalion

AIR ASSAULT!

FORT DRUM, N.Y. – Soldiers from the 11th Cyber Battalion, SSG Antonio Borden-Colvin, C Company; SGT Isiah Nembhard, Headquarters and Headquarters Company; and SPC Alexander Rivera Santiago, A Company, recently graduated from the 10th Mountain Light Fighter School's Air Assault Course. These three CEMA Warriors are also members of the U.S. Army Cyber Command Best Squad that will represent ARCYBER in the Army Best Squad Competition from September 24 through October 6. Congratulations to SSG Borden, SGT Nembhard, and SPC Rivera on their amazing accomplishment. They continue to demonstrate what it means to be LEVIATHAN STRONG! GLOBAL REACH, GLOBAL IMPACT! (Courtesy Photos)

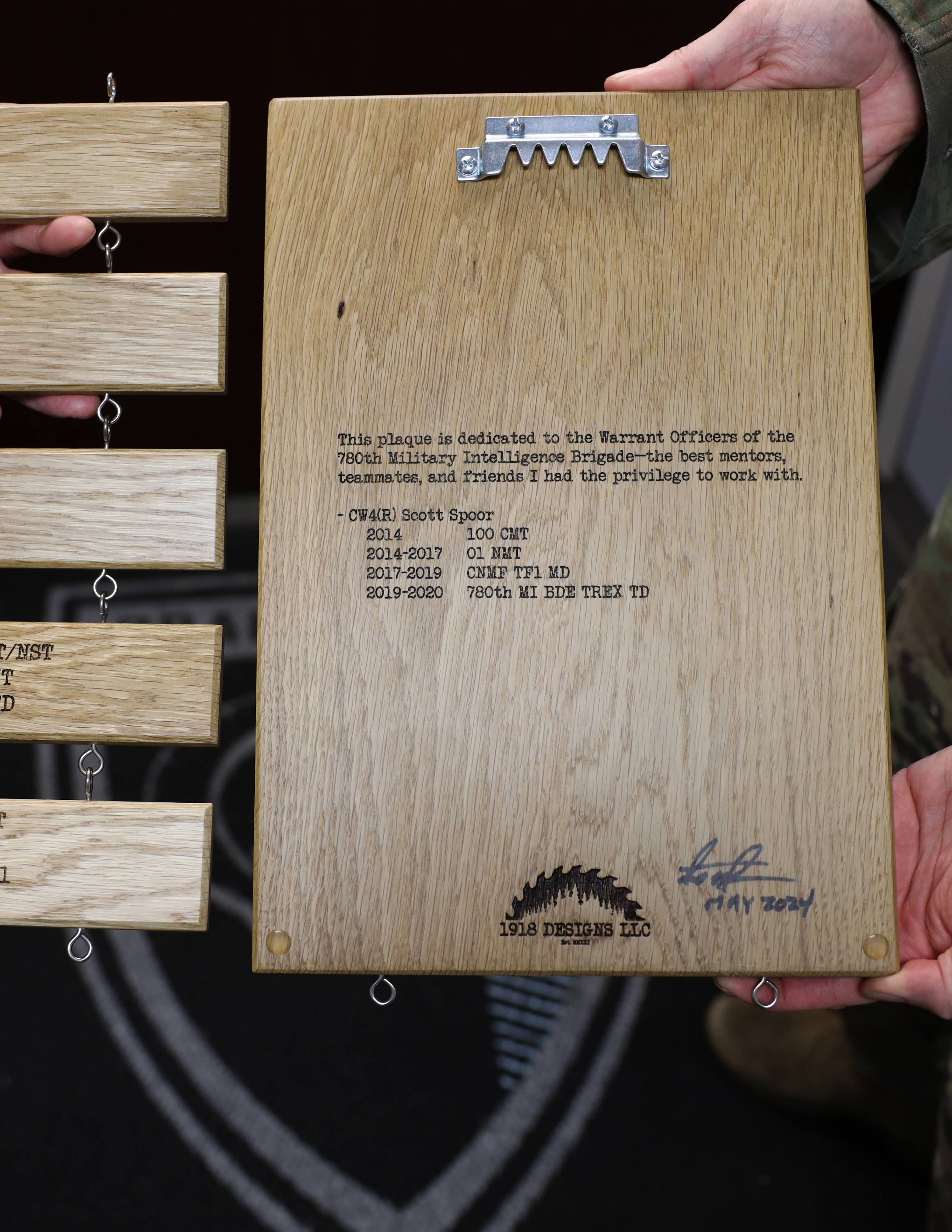
LEADERSHIP MATTERS! FITNESS MATTERS! WINNING MATTERS!

FORT EISENHOWER, Ga. – Leaders in Apex Company demonstrate how Soldiers in the 11th Cyber Battalion become LEVIATHAN STRONG! Train hard, fight hard, win easy! GLOBAL REACH, GLOBAL IMPACT! (Courtesy Photos)

TRAIN HARD, FIGHT HARD, WIN EASY!

FORT EISENHOWER, Ga. *– Leviathans from Apex Company, 11th Cyber Battalion, executed a 72-hour CEMA focused field training exercise in extreme weather conditions to prepare for their upcoming Joint Pacific Multinational Readiness Center 25-01 rotation. Apex will be supporting 25th Infantry Division during the rotation. LEVIATHAN STRONG! GLOBAL REACH, GLOBAL IMPACT! (Courtesy Photos)*

2013-2016 61 NMT
2018-2019 101 CM
2019-2020 JMOC T
2014-2015 23 N-CPT
2015-2018 61 NMT
2018-2020 CNMF TF
2020-2022 USCC MD



This plaque is dedicated to the Warrant Officers of the 780th Military Intelligence Brigade—the best mentors, teammates, and friends I had the privilege to work with.

- CW4(R) Scott Spoor

2014	100 CMT
2014-2017	01 NMT
2017-2019	CNMF TF1 MD
2019-2020	780th MI BDE TREX TD

1918 DESIGNS LLC
Est. MMXXI

MAY 2024

NEXT QUARTER'S BYTE IS focused on the Brigade's Civilians. As in other issues of the BYTE magazine, the command encourages your contribution to drive the Cyber and Information Advantage conversation. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT November 15, 2024. Final articles are due November 29.

THIS IS THE WAY
CW5 AL MOLLENKOPF - 2011-2014
CW5 JOHN O'REILLY - 2014-2018
CW5 TRAVIS YSEN - 2018-2020
CW4 ERIN WARD - 2020-2022
CW5 JAMES RICHARDS - 2022-2025