



Network Enterprise Technology Command

NETCOM

2023



The MERCURY



WHATS INSIDE THIS ISSUE

CONTRIBUTING UNITS

NETCOM G1	106th
NETCOM G5	55th SIG CO
NETCOM G6	93rd
DSD	RCC-K
CSD	21st SIG BDE
	CPB
	B/392

The Network Enterprise Technology Command (NETCOM) The Mercury is an authorized publication for members of the U. S. Army NETCOM Team, and its subordinate commands and organizations throughout the world, in accordance with AR 360-1. Contents of The Mercury are not necessarily the official views of, or endorsed by, the U.S. Government, the DoD, U.S. Army, U.S. Army Cyber (ARCYBER) or NETCOM.

The design and editorial content of this publication is the responsibility of the NETCOM Public Affairs Office (PAO). To contact the NETCOM PAO, call (520) 227-4299 or email usarmy.huachuca.NETCOM.mbx.hq-pao@army.mil. The mailing address is: ATTN NETC-PA (PAO), USA NETCOM, 2133 Cushing Street, Suite 3209, Fort Huachuca, AZ 85613-7070.

Command and Editorial Staff

Commanding General - MG Christopher L. Eubank
Deputy Chief of Staff - Matthew W. Barker
Chief, Public Affairs - Gordon Van Vleet
Managing Editor - Sharon K. Shulsky
Co-Managing Editor - SFC Kelvin P. Ringold
Designer/Multimedia Officer - Amanda D. Pearson

Insights from the CG MG Christopher L. Eubank

Greetings to Team NETCOM. I first want to thank each of you for what you do to ensure the NETCOM mission is accomplished to standard in support of the Army every day. I am going to use this message to lay out some thoughts I have about NETCOM as an organization today, what we have done over the last year and where I think we are headed over the next year.

First, who are we as an organization? I believe that we are the premiere communications organization in the Army, and I dare say the Department of Defense. We are a two-star operational command with global responsibilities that is in competition, crisis, and conflict 24/7/365. We enable decision dominance across the globe to our customers by delivering information technology services and allowing access to data at the point of need to ensure mission command can be executed in support of missions. This is all possible because of the world class workforce inside of the NETCOM enterprise. I am in awe of each and everyone in this formation and what you do to ensure that the Army operates and conducts its mission in defense of the nation. People are our most treasured resource, and I am thankful for all of you for which I am honored to serve.

The last year has moved by very rapidly and along with operating and maintaining the Army's portion of the DOD Information Network daily this team has pushed the Army closer to a unified network based on zero trust principles than any other organization. This has been done through a concerted effort across the command from the Regional

Cyber Centers rolling out new capability globally to managing the Army 365 tenant daily to the G7s working on building out organizations to support expansion in Europe; the entire team has been involved in improving the network in support of the Army of 2030. On top of this, we have worked hard to convert the workforce to Cyber Excepted Service which brings additional benefits to team. This year was full of accomplishments, such as rolling out Azure Virtual Desktop in support of teleworking, mobility, and remote work as well as the potential to deliver services to the National Guard and Army Reserves in a more secure, reliable, efficient, and just as effective manner. The use of personal devices to access the Army 365 resources was rolled out, and we were able to allow the first test users to seamlessly move and log into their resources with the Army Unified Directory Services pilot. Moreover, we welcomed our first set of intelligence professionals to the RCCs, which is enhancing our intelligence analysis of the cyberspace domain even further. There are so many more initiatives and accomplishments, but suffice it to say, we have been busy improving the network while running it daily.

The priorities for the next year remain the same as we look to continue to build upon the capabilities we have put in place with an eye on improving the classified networks. This includes setting the conditions to enable the use of an Office 365 environment while modernizing the network to use more commercial platforms. As we work to set the network, we will continue to strive to reach full operating capability on the Global Cyber Center

Command Sergeant Major Jason D. McCoy answers the question:

What does the phrase "This is NETCOM" mean to you?

As I walk around the NETCOM footprint, both at Fort Huachuca and abroad, I am continuously impressed by the professional excellence of our team. However, I constantly ask myself if I am doing enough to improve the lives of those that inspire me. An important part of leadership is acknowledging that we must continuously improve to positively affect the lives and experiences of our Soldiers, Civilians, and Families. For example, if you look around Greely Hall, we are continuing to transform our headquarters for the betterment of our workforce based on input from those that work here.

People will always be a priority. I think it is important for leaders to look around and ask ourselves, "how can we transform NETCOM to be the best version of itself?" I believe it is critical for leaders to have open, candid discussions with everyone on how we can take a commonsense approach to improve NETCOM. We need to take a step back and ask ourselves, "we know we are doing the right things, but are we doing those things the right way?"

As we began 2023, we assessed how we could better utilize existing technology to not only benefit NETCOM, but also the Army as a whole. For NETCOM, we needed to support on-going and future Army strategies such as the Army's Finance Strategy 2026 and Department of Defense Sustainability efforts. One example of our transformation efforts focused on reducing printing costs by utilizing Quick Response (QR) codes and virtual documentation. This effort alone saved us approximately \$1.2 million a year by reducing costs associated with printing. Funds which we can utilize in other areas to benefit the overall mission.

Focusing on the Army's Digital Transformation Strategy, NETCOM leads the Department of Defense's Zero Trust efforts by implementing user-friendly and secure collaborative platforms like Army 365. The Army 365 platform replaced the Defense Enterprise Email and introduced collaborative tools like Teams and Office 365 that remote and mobile devices can access through the

Department of Defense Information Network – Army. Modernization efforts, such as Army 365, streamline the services we provide and reduce costs associated with maintaining duplicative services and capabilities. Innovation like this continues to show NETCOM's dedication to embracing continuous improvement and will help improve how the Army communicates.

This transformation mindset is at the heart of "This is NETCOM!!". We set the standard through constant innovation for ourselves and our customers. We look not to the past, but to the future. Throughout this publication are examples of how our dedicated team of consummate professionals realize that goal. Yet, we must not rest on our laurels as we have more work ahead.

As we continue to transform our organization to support the Army of 2030, it is crucial we continue to focus on our support to modernization, and how it can help

How NETCOM Leads the Army to a Zero-Trust Network

Mr. Patrick C. Dedham

Deputy to the Commanding General



Zero-Trust is a collection of concepts and ideas that assume no trust exists within a defined enterprise network. The Network Enterprise Technology Command (NETCOM) - Army Department of Defense Information Networks (DoDIN-A) Cybersecurity Strategy uses Zero-Trust principals to protect critical Data, Applications, Assets, and Services (DAAS). The strategy moves defenses from static network-based perimeters to focus on users, assets, and resources. Organizations without a Zero-Trust architecture may risk dangerous cyber-attacks. Zero-Trust aims to verify every user, validate every device, and smartly limit access to DAAS.

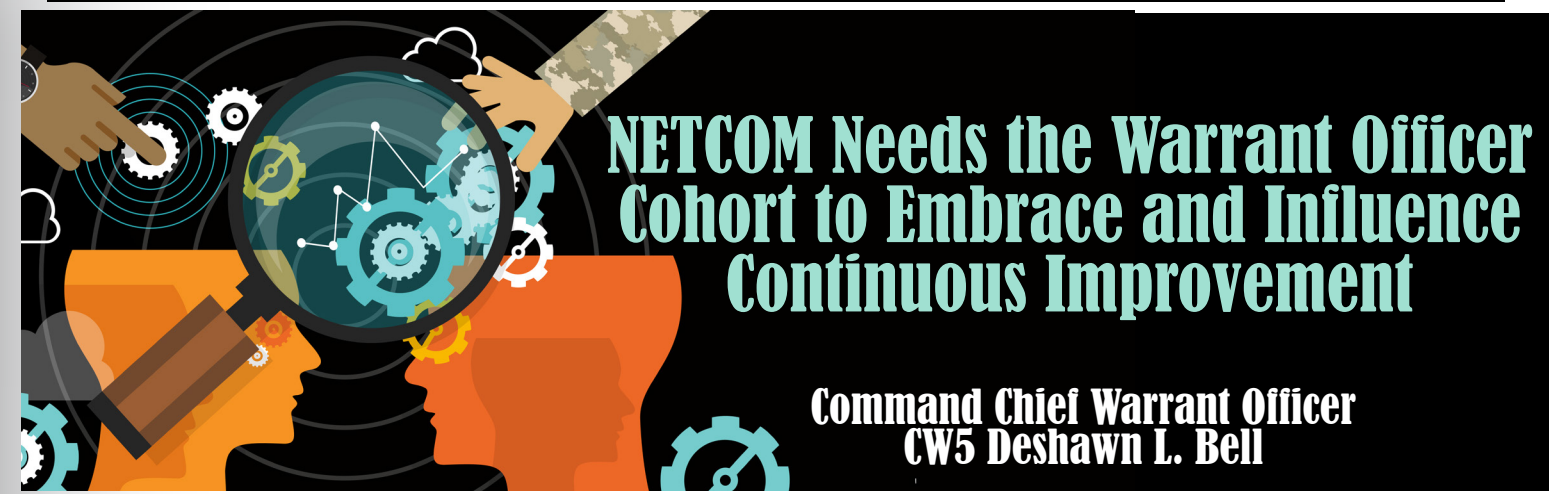
NETCOM is leading several continuous improvement projects for the Army to achieve a Zero-Trust network that only allows enterprise organization's account-based users access once authorized and authenticated. The security architecture uses the Zero-Trust seven pillars: user, device, network, visibility and analytics, automation and orchestration, application and workload, and data. A more robust user identification and access policy, continuous monitoring of users and devices, network segmentation to prevent lateral movement, strong data security in transit and at rest, and automated security response achieve a Zero-Trust security architecture.

NETCOM's end state is to have a DoDIN-A based on Zero-Trust principles that treats every system connection and endpoint as a threat using four main premises: log and inspect all internal and external traffic, control attempted access to networks, keep network resources secure, and verify all sources and resources. Users must authenticate their iden-

tity before Zero-Trust permits granular access. The Zero-Trust framework differs from virtual private networks (VPNs) and internet-based cloud access as it does not grant access to all data. Zero-Trust offers a least-privilege access approach, occurring for every connection. The NETCOM Zero-Trust architecture will give access to a user on a limited-time basis, under the right circumstances, and after user authentication. It only grants access to data needed for the user to complete their task.

NETCOM conducted a gap analysis on current Department of Defense and Army capabilities to inform related technology decisions and implementation for operationalizing the Army Zero-Trust architecture. NETCOM utilized the Cybersecurity Strategy's core concepts as the criteria for the analysis. The gap analysis identified 26 unique gaps across the dependencies of the seven Zero-Trust pillars previously mentioned. Policy or configuration changes could mitigate some independent gaps at any time, while several others fall into four main groups. The four key categories recommended in mitigation priority are internet-accessible endpoint management and security, standardized and secure access to hybrid resources, granular data access control and logging, aggregation, automation, and orchestration. This path forward guides the Army toward initiating a holistic set of solutions to enable a Zero-Trust framework.

The Army's end state is to ensure secure information at all operational levels, providing users with access to required resources from any device from any location. The way for the Army to achieve its



As the Army adapts to changes in technology and enemy capabilities, highly specialized experts and trainers will be needed to help incorporate and maintain cutting-edge technologies to enable mission success for the Army of 2030. Looking towards the future, those technical experts are led by the Warrant Officer Cohort. The NETCOM family has a lot of warrants who continue to demonstrate high performance and a great potential, but we cannot rest...because our nation's adversaries are not resting. We must understand NETCOM's vital role driving DoDIN Operations across the Army to enable our leaders to have decision dominance over our nation's adversaries. We must embrace and realize that this is not your father or mother's NETCOM.

As highly trained experts we are the advisors in our organizations. As such, warrant officers must have a seat at the table. It is crucial that warrant officers understand t we must be an integral part of the commanders' and directors' decision-making process. Warrant officers will undoubtedly experience commanders and directors that do not fully leverage their warrant officers, so this is

when the warrant officer leans on his/her experience and self-confidence. Make a point to inject yourselves if you are not previously invited into critical discussions. Make your presence known, by words and actions, that you are an indispensable member of the team. I have no doubt your boss will welcome your proactive actions to be included. In fact, it is expected! We all specialize in some of the most critical technical areas in the Army, so we owe it to our commanders and directors to show our value and show how our presence positively influence the positive evolution of the DoDIN in support of the greater Army mission.

To this end, the warrant officer, as the technical expert and advisor, must understand NETCOM's operational and strategic mission. We must advise and support the commander's and director's direction and goals. To do that, we must be an integral part of the command.


To truly be integral, we must also lead! As warrant officers, we have the responsibility to also utilize our own leadership skills. Training our future technical experts and leaders is always one of our most important jobs – mentorship (up and down) is a cornerstone of who we are. Being a technical expert, problem




“Season is a wise metaphor for the movement of life, I think. It suggests that life is neither a battlefield nor a game of change but something infinity richer, more promising, more real.”
- Parker J. Palmer, *Let Your Life Speak*

Lines of Effort

- 1 People** Recruit, Develop, Manage and Retain a Highly Qualified and Agile Workforce; Cultivate innovative, adaptive resourceful, motivated and selfless professionals.
- 2 Readiness** Conduct effective DoDIN-A operations; Resource the Network; Execute effective compliance and inspection programs; Conduct NETCOM Mission Command.
- 3 Continuous Improvement** Optimize the Network and IT Services; Continuously improve to achieve a Unified Network.

 NETCOM leads global operations for the Army's portion of the DoDIN, ensuring freedom of action in cyberspace while denying the same to our adversaries in support of multi-domain operations.

 NETCOM 2030 is the premier communications organization and information services provider to all DoDIN-Army customers worldwide, ensuring all commanders have decision advantage in support of mission command within the multi-domain environment.

 usarmy.huachuca.NETCOM.mbx.hq-pao@army.mil

 <https://www.facebook.com/USARMYNETCOM>

 <https://www.flickr.com/photos/usarmynetcom>

 <https://www.linkedin.com/company/us-army-network-enterprise-technology-command>

 <https://netcom.army.mil>

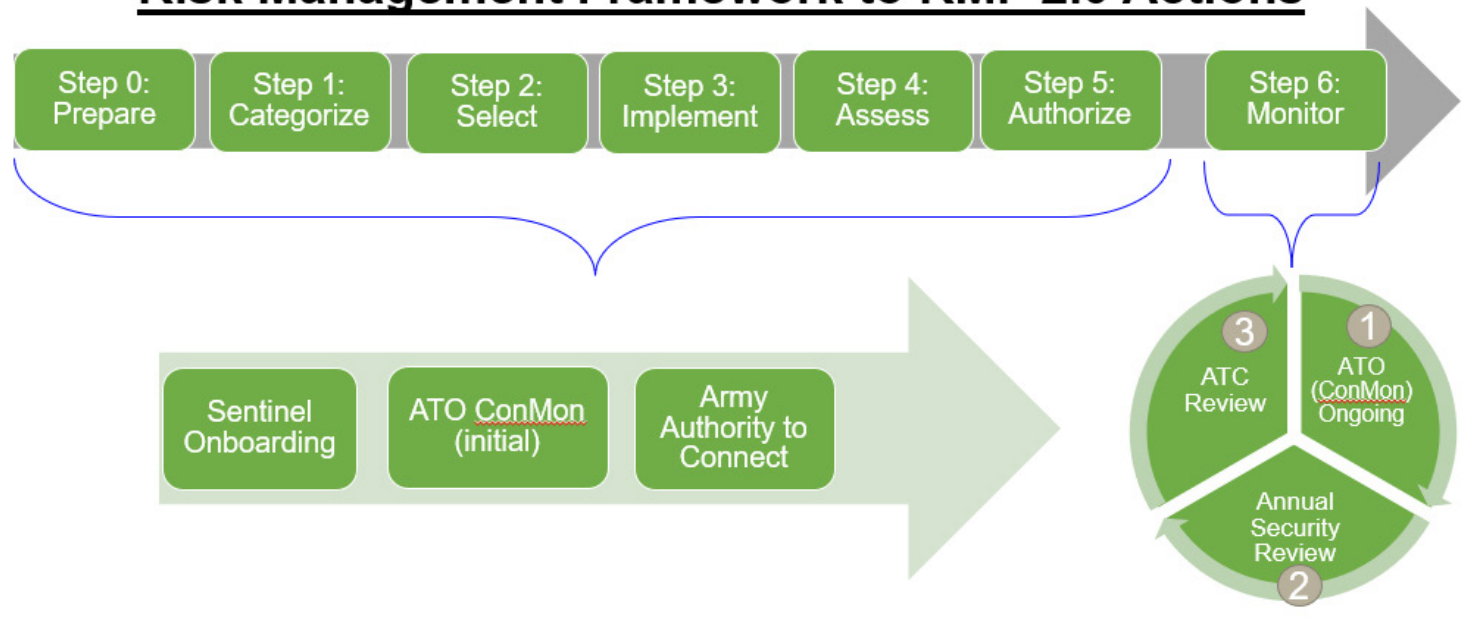
Risk Management Framework (RMF) 2.0

- By Joseph L. Valladares, Director Cybersecurity Directorate (CSD)

The U.S. Army Network Enterprise Technology Command (NETCOM) is leading the way in operationalizing cybersecurity reform through a revolutionary effort known as RMF 2.0. Under this refined cybersecurity activity, the Army is focusing on the “right” security controls to ensure our cyber capabilities continue to support our warfighters in the highly contested cyber domain. The focus is ensuring we are securing our systems, applications, and networks. The corner stone of the RMF 2.0 is the implementation of an Enterprise Common Control Provider (CCP) known as the Army Sentinel CCP. This CCP provides security control inheritance for all Army cyber capabilities where many security objectives are covered at either the Army or DoD level, through policy and regulation. As equally important, is the implementation of the Army Authority to Connect (ATC) process whereby a small number of appointed Network Authorizing Officials (NAO) will be provided a holistic risk assessment for cyber

capabilities operating on the Army’s portion of the Department of Defense Information Network (DoDIN-A) in order to approve continued connection and operation. The foundational aspect of the Army ATC process is first and foremost to ensure defensive oversight for everything on the wire. Rounding out these foundational aspects of RMF 2.0 is the shift to Continuous Monitoring (ConMon), whereby commands and organizations responsible for the operation of cyber capabilities will move into an annual security review process that ensures not only continued validation of critical security requirements, but also fulfills the Army’s obligation under the Federal Information Security Modernization Act (FISMA). The NETCOM Cybersecurity Directorate (CSD) is wholly responsible for documenting all operational processes, training the Army cyber workforce, ensuring governance and oversight, and performing risk assessments as the Army’s Control Assessor.

Risk Management Framework to RMF 2.0 Actions



There is increasingly steep global competition for the best candidates across the entire hiring spectrum both within and outside of the Federal Government. The Science, Technology, Engineering and Math (STEM) fields continue to grow at a much faster rate compared to the growth rate of other professions, therefore increasing the demand for STEM graduates. With STEM occupations in high demand, NETCOM is taking measured steps to establish an outreach program strategy to help attract qualified employees. Outreach and recruitment techniques change over time. As a result, NETCOM G-1/Talent Management are developing new ways to attract and retain talent in the form of agile outreach and recruiting practices. NETCOM’s agile methodology encourages a shift away from rigid processes and fixed timescales to more responsive, real-time outreach and recruiting practices geared towards the new, virtual talent marketplace. NETCOM G-1/Talent Management is implementing agile outreach and recruiting practices that adopt modernized outreach and techniques that include: leveraging Direct Hire (DH) where applicable, considering Over-hire options where DH not authorized (i.e. DCIPS), encouraging employees to inform G-1 of retirement intent in order to plan Talent Acquisition, collaborate on new processes within G-1/Talent Management to advertise vacancies on social media platforms, and inform Talent Management Acquire team of recruitment opportunities unique to field/job series. NETCOM G-1/Talent Management is engaged in building awareness about NETCOM’s mission and identity across industry events and media platforms, i.e. Cyber Summit-TechEx-pousa.com, Yello, and LinkedIn.

NETCOM G-1/Talent Management, in partnership with NETCOM’s Data Science Directorate (DSD) is analyzing data available from federal and industry resources i.e. Federal Employee Viewpoint Survey (FEVS), Defense Manpower Data Center (DMDC), Force Management System Website FMSWeb), and LinkedIn analytics that provides information regarding the current workforce across mission critical occupations, including demographic and background characteristics of the current workforce, retirement eligibility, turnover, and various workforce management issues (i.e., recruitment and retention). This information is valuable in understanding the workforce across the organization and identifying trends impacting the workforce as a whole or in part. It informs workforce and succession planning by providing a basis for action to address demographic and employment trends that may impact future mission capabilities. The CG’s vision contained in NETCOM’s Strategic Human Capital Plan (SHCP) produced by NETCOM G-1/Talent Management lays out the way forward to acquire, develop, employ and retain the NETCOM workforce. In addition, NETCOM G-1/Talent Management is developing a strong partnership with Army Civilian Career Management Activity (AC-CMA) in support of improved workforce planning accuracy and improved capabilities to match anticipated growth with talent acquisition. This strategic alliance will better enable NETCOM to manage critical workforce competencies by incorporating new methods to introduce key skill sets into our hiring and development processes.

Data-Driven Decision Making & NETCOM's Data Science Directorate

- By Kevin Goulding, NETCOM DSD (Pittsburgh)



True to its name, Data-Driven Decision Making (DDDM) is the concept of using measurable data to guide strategic decisions. For a data-rich organization like NETCOM, there are countless opportunities to employ DDDM, and the Data Science Directorate (DSD) is uniquely trained and positioned to do so. Dispersed across four geographic locations, DSD made significant headway throughout 2022 on a varied project portfolio.

Co-located with NETCOM HQ at Fort Huachuca, DSD's Network Operations and Analysis Division (NOAD) efforts focused on making existing data more accessible and included the following projects:

- NOAD developed a web-based dashboard for unit command teams that used existing personnel data to display retirement projections, and it developed a predictive model to forecast impending retirements and associated risks.
- In support of the effort to build out the Army's Big Data Platform, NOAD worked with ARCYBER to develop parsers that would assist with data storage of authoritative data sources in conjunction with the development of a consolidated data science environment facilitating project work, data sharing in near real time, and asset visibility.
- NOAD worked the NETCOM effort to optimize IPv6 address assignment for the DoD through autonomous algorithms in order to better define ownership, type of device, location, etc.

Just north of Fort Huachuca, DSD's Phoenix-based Data Science Centers (DSC), used its ample data supply on two of its own DDDM efforts:

- After the Log4j/Log4Shell vulnerability wreaked havoc in late 2021, DSC-Phoenix conducted post-mortem analysis of its effects on the DOD network, supporting defense-in-depth network operations decisions.
- Additionally, DSC-Phoenix conducted a feature extraction/engineering effort to support network switch/router performance decisions.

Out west, DSC-Monterey leveraged its proximity to both the USMC and the Naval Postgraduate School to field-test its work, and it contributed to improving NETCOM's data infrastructure:

- The USMC utilized NETCOM's Army Network Information Management Environment (ANIME) network and sensor information in real-time decision making to enable fires de-conflict and during a fires exercise at 29 Palms.
- DSC-Monterey supported G26's exploration of various data platforms, to include ThreatQ, MITRE OpenCTI, and the Malware Information Sharing Platform (MISP). These close efforts guided the ongoing effort to modernize the storage and distribution of threat intel data.
- DSC-Monterey conducted network flow analysis to provide insight to normal/ anomalous network behavior to enable real-time TTPs to be developed and implemented for network management i.e., Software-Defined Network (SDN) behavior.

Finally, DSC-Pittsburgh worked with Carnegie Mellon University, and its Software Engineering Institute (SEI), on a wide variety of DDDM-flavored projects:

- Following the high-profile leakage of a senior Army officer's official emails, DSC-Pittsburgh performed Natural Language Processing (NLP) analysis to identify any instances of leaked PII.
- DSC-Pittsburgh served as a tool champion and advisor in ARCYBER-led efforts to visualize and inventory assets connecting to the DoDIN. The effort consists of a prototype, interim solution that merges big data from a legacy system to inform a Power BI dashboard

Future of Army Networks and NETCOM

- By Robert L. Snell, G5 NETCOM

If we need assistance with personnel actions, we go to G1. When our computers are not working correctly, we go to our Information Management Officer and G6. If we have questions about funding, we talk to G8. But who do we talk to about the future of the Army networks and the role NETCOM has in this vision?

NETCOM G5 is instrumental in the future planning efforts for NETCOM's 2030 Vision as the premier communications organization and information services provider to all Department of Defense Information Network-Army (DoDIN-A) customers worldwide. Meeting that mission is essential to the success of the DoDIN-A, by ensuring NETCOM is enabling all commanders with decision advantage in support of mission command while operating in a multi-domain environment.

Fundamentally, the G5 team researches and develops strategies to help NETCOM, and the Army, better support the Warfighter. They are instrumental in executing the planning efforts on behalf of the DoDIN-A, enabling the Area of Operations Commander.

Below are the Enterprise capabilities and initiatives the G5 is working on behalf of NETCOM:

Implementation of Commercial Solutions for Classified (CSfC)- Virtual Secure Remote (ViSR) solution as part of the Coronavirus Disease 2019 (COVID19) response provided Army users with Secret Internet Protocol (IP) Router Network (SIPR-Net) regionalized secure access remotely as well as through the DOD Information Network (DoDIN).

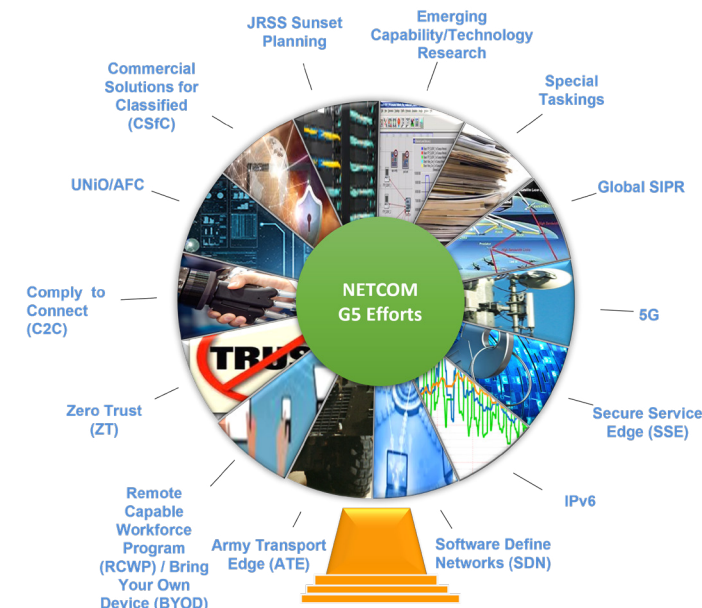
This CSfC capability installed at Fort Liberty, NC is known as ViSR. It initially supported remote SIPRNet access for up to 2,000 users but is scalable up to 15,000 concurrent users as the Government continues to onboard users.

As part of this initiative, the Army is also installing a CSfC/VDI capability in the Hawaii Schofield Barracks and Fort Shafter locations under United States Army Pacific (USARPAC). The USARPAC CSfC capability, equipment initially supported 2,000 users, with space to expand the infrastructure to support additional users in the future.

Modernizing the SIPR-Net leveraging CSfC in conjunction with Virtual Desktop Infrastructure (VDI)/Multiple Independent Levels of Security (MILS) to build an integrated enterprise SIPRNet environment simplifies operations through the centralization of data, resources, and security mechanisms; while enhancing mobility; and providing operational flexibility. The Army is moving

away from the use of network-based security stacks and the hosting of installation centric services and security by looking towards enterprise level cloud and data center hosted services and security models. To the extent possible, Army will divest aging SIPR-Net Top-Level Architecture (S-TLA) stacks.

Comply to Connect (C2C)- The National Defense Authorization Act (NDAA) FY2017 § 1653 requires that DoD Components and Services identify and report all devices connected to their respective DoDIN networks. The implementation of C2C is a Cyber Security framework that addresses this NDAA requirement. The framework consists of 5 steps: 1) discover, identify, and categorize endpoints, 2) interrogate the



2022 Vulnerability Disclosure Program

Year in Review

- By Joseph L. Valladares, Director Cybersecurity Directorate (CSD)



2022 was another exciting time for the Army's Vulnerability Disclosure Program and if the numbers tell us anything when compared against 2021 – we are getting better at locking our front door, but we keep forgetting our mail on the front porch. What does this mean?

The number of actionable reports, submitted by researchers across the globe fell by 32%! We reduced the number of vulnerabilities from 2021 to 2022. Vulnerabilities ranging from SQL Injection and Cross-Site Scripting to our all-time favorite, Information Disclosure (this is where the mail on the front porch issue comes in). To quickly frame what's included in the VDP – it is anything and everything Army related that is publicly accessible from a commercial connection. Websites, VPNs, commercial repositories such as GitHub and Amazon S3 Buckets as well as

our social media pages. If the Army is using it, and it has Army information there – hunting season is open.

Information Disclosure, tracked as CWE-200 within the Common Weakness Enumeration catalogue (<https://cwe.mitre.org/>) is the Exposure of Sensitive Information to An Unauthorized Actor. This category, while it encompasses a lot, impacts the Army in a few ways; CUI/FOUO documents are accessible to anyone on the internet without authentication, webserver information is disclosed within HTTP Headers and default server pages are still present on a website. While we did have a few reports in 2022 (two, to be exact) that were critical in nature (compared to the five in 2021), the majority of our 2022 Information Disclosure issues were Medium (47) and Low (211).

For 2023, let's keep pushing the number of actionable reports that come into the VDP, down. If you are an application or web developer, you should already have the Open Worldwide Application Security Project (OWASP) website bookmarked (<https://owasp.org/www-project-top-ten/>). Leverage the Top 10 list as your self-assessment checklist. Make sure you are taking the simple steps to not disclose server information, protect your web.config and httpd.conf files. Most of all, if you have a public site hosting CUI/FOUO documents; make sure it requires authentication prior to gaining access!

When in doubt, and if you need guidance, do not hesitate. Reach out to the NETCOM Cybersecurity Directorate. We'd be happy to get you going down the right path to greatness, and better website security.



GEARS Transitions to the Cloud at Army

- By Bill Sherod, Chief, Projects & Development Division G6

NETCOM's Global Electronic Approval and Routing System (GEARS) has been in existence for over 10 years and has grown from an internal NETCOM HQ routing tool to an enterprise capability that serves customers across the DoD to expedite the processing of administrative actions. Last year GEARS processed over 1.8M packets and served over 250K discrete users.

GEARS 5 was hosted on the DISA Defense Enterprise Portal System (DEPS) and was SharePoint based. These limitations coupled with the volume of packets being processed required the NETCOM G6 to develop a cutting-edge capability that meets the needs of our expanding customer base. The GEARS 6 application was completely re-written from scratch as a cloud-based Platform as a Service (PaaS) tool and eliminated the size and object limitations of SharePoint.

At the same time the GEARS 6 application was being developed, the transition to a new hosting platform was also required. Army

365 and the Army's Cloud Plan for cloud hosting were coming on board and the Army would no longer use DISA DEPS as a hosting platform. One of the most significant challenges to this project was the development and deployment of the new GEARS 6 capability into a new cloud environment called cARMY. The Army's cloud environment was still maturing, and the G6 Team worked hand in hand with cARMY technicians and the Enterprise Cloud Management Agency (ECMA) to overcome many obstacles and 'paved the way' in fielding GEARS 6 as the first PaaS capability in the Microsoft Azure cARMY production environment. The G6 team had to perform extensive coordination, exploration, troubleshooting, and refinement with multiple external organizations to ensure user identity, platform, and other services all came together to have GEARS 6 functional within required timelines. GEARS 6 is also the first PaaS application in cARMY that has DoD-Wide identity and authentication feeds directly from the DISA Global Federated User

Domain (GFUD). This capability allows all customers across the DoD to access and use GEARS with CAC authentication.

GEARS 6 fully leverages cloud technology for scalability and optimizes the application's resources for performance during periods of heavy use. GEARS 6 also streamlines workflows to reduce stuck packets, which was an issue with the SharePoint GEARS 5 version. These features improve the GEARS user experience and the G6 team continues to improve the application by adding features and capability based on user feedback. Several significant enhancements are already in the works such as the ability to sign documents within the application without downloading and the ability to dynamically change a packet route. NETCOM G6 is proud and thankful for the exceptional collaboration and effort from NETCOM G6 DAC and contractor staff, ECMA, Microsoft, DISA, and other organizations throughout this project.

Continued from Zero Trust...

end state involves continuous improvement, optimization, and integration of an Army Unified Network to achieve Zero-Trust target levels by 2027. Bi-weekly Army Cyber Command and NETCOM-led Continuous Improvement Activities Board synchronizes and manages all Zero-Trust related enterprise efforts. Soon this effort will expand to include the Tactical Edge. NETCOM is performing many activities to achieve or support

DOD Zero-Trust capabilities, including a Security Service Edge Crosswalk, improving Army Endpoint Security System (AESS), integrating Microsoft Defender for Endpoint (MDE) and Office (MDO), implementation of Army Unified Directory Services (AUDS), Unified Security Information and Event Management (U-SIEM) implementation, as well as executing Data Tagging for Data Loss Prevention and Digital Rights Management.



Photo credit – (Top left): Mr. Steven Dinote, U.S. Armed Forces Sports Photo credit – (Top right & bottom left): Mrs. Shatara Riis, CPB Public Affairs

Cyber Protection Brigade Soldier Aids All-Army Soccer Team in Championship Win

Named to All-Tournament Team in 2023 Armed Forces Men’s Soccer Championship

- By Shatara Riis, Cyber Protection Brigade

Sgt. Ivan Oseguera, a Soldier assigned to the 60th Signal Battalion (Offensive Cyber Operations), represented the Cyber Protection Brigade as a member of the All-Army Soccer Team. Oseguera and the All-Army Soccer Team claimed the championship trophy in a close out bout against the Marine Corps winning the 2023 Armed Forces Men’s Soccer Championship held

at the Paige Fieldhouse Marine Corps Base Camp Pendleton, California, April 11, 2023. The All-Army Soccer Team dominated the tournament in a four-game sweep. Sgt. Oseguera was selected to the All-Tournament Team. Sgt. Oseguera is a native of Yuba City, California. He enlisted in the Army in January of 2019 as a 25B, Information Technology Specialist.

Greely Hall - Home of NETCOM HQ

FACTS ABOUT GREELY HALL

- Built 1950's - originally designated as a research facility
- Named after the late Maj. Gen. Adolphus Greely
- Considered a historic structure
- Today - serves as an administrative building with a data center, courtroom, auditorium, operational spaces, etc.

Continued from Civilian Talent...

Career Fairs and Virtual Outreach are another major initiative currently underway between NETCOM G-1/Talent Management and with the newly formed ARCYBER Talent Management Division to include NETCOM representation at future career fairs by helping to communicate career fair events to potential NETCOM participants and assist ARCYBER with estimating funding and cost information pertaining to NETCOM’s participation. In addition, NETCOM G-1/Talent Management has produced and distributed a Virtual Outreach SOP containing tools, techniques, and lessons-learned from NETCOM’s participation in previous Career Fairs.

During the past calendar year, NETCOM participated in and was represented at several academic outreach events that included: the University of Arizona (Virtual Career Fair), Carnegie Mellon (STEM Career Fair) in Pittsburgh, PA, University of South Carolina (STEM Career Fair), University of Texas (Fall 2022 Technology & Sciences Virtual Career Fair), Dakota State University (Career and Internship Career Fair), and NETCOM plans to participate in similar future outreach and recruiting events.

NETCOM also participates in the Army Career Exploration, Advancement and Development (CEAD) Program. CEAD provides summer internships and full-time internship opportunities with the goal of converting high-quality interns into permanent employees.

In addition, NETCOM actively participates alongside our parent command and the Army Digital Transformation team to introduce capability to build and maintain competencies in a Learning Management System to close skill gaps across NETCOM and the larger Army digital technology footprint. NETCOM G-1/Talent Management is also providing input to the Army Learning Management System (ALMS) user interface redesign that include features and functionality; skills assessment; and learning capabilities to provide new skills in our IT workforce that attract and incentivize our workforce to start gaining the skills that we want them to have for the future.

“ An empowered organization is one in which individuals have the knowledge skill, desire, and opportunity to personally succeed in a way that leads to collective organizational success. ”

- Stephen Covey

The Science, Technology, Engineering and Math (STEM) fields continue to grow at a much faster rate compared to the growth rate of other professions. NETCOM continues to experience challenges associated with building bench strength at a time when there is increasingly steep global competition for the best candidates across the entire employment and retention spectrum. NETCOM G-1/Talent Management remains committed to building relationships with industry and academia and adopting workforce management technology and tools that transform the way NETCOM acquires, develops, employs, and retains its’ civilian workforce of the future.

55th Combat Camera

Documenting History in the Making

- By Colin Broadstone, 7th SC(T) PAO

FORT MEADE, MD. – The U.S. Army’s 55th Signal Company, also known as Combat Camera, has long been at the forefront of documenting the Army experience across the globe. The only active-duty Combat Camera unit, the 55th deploys worldwide with Army units to provide still and video documentation of Army operations during peacetime, contingencies, and combat.

The vital work of the 55th Combat Camera supports commanders’ tactical, operational, and strategic objectives—and provides the public a window into the world of the Army. The talented Soldiers of the 55th document history in the making; in doing so, they also help build the Army of the future by aiding recruitment and retention efforts.

In one of their most notable deployments of the past year, the 55th Signal Company provided support to Army units during AFRICOM’s Flintlock training exercise held in March of 2023. Flintlock strengthens the ability of key partner nations in the region to counter violent extremist organizations, collaborate across borders, and provide security for their citizens, while building trust with civilian populations.

Staff Sgt. Alexander Nieves, a squad leader in 1st platoon, re-enlisted in August 2022. He is typically responsible for the well-being of nine Soldiers in the company, preparing them for upcoming missions. Staff Sgt. Nieves was the NCOIC for the Flintlock deployment, leading six Soldiers to document the exercise alongside the Air Force Combat Camera.

“Flintlock was the first time that I’ve gone overseas since 2015,” said Nieves. “We had a team of six Soldiers and were in addition to the Air Force Combat Camera in documenting the entire exercise.”

During this exercise, Staff Sgt. Nieves served primarily as photographer, but said the whole experience was transformative for him as he worked with diverse professionals from all over the world. He was able to lead documentation planning efforts and conduct briefings, and created scores of photos and videos for social media and unit use.

Staff Sgt. Charles Brock Jr., the visual information manager for 4th platoon, assisted Nieves in his efforts at Flintlock, and said their experience demonstrated the value of international camaraderie in military operations.

“What stood out to me to see was how fast we built a partnership in three weeks,” said Staff Sgt. Brock. “Everywhere you go, there’s a different story, there are stories that people haven’t heard of. When we’re out there taking these pictures, we are telling a story and giving it to the American public.”

Another deployment the 55th Signal Company undertook this past year was for Operation Inherent Resolve. Sgt. Julio Hernandez, a former military police officer who transitioned to the 55th as a Combat Camera Specialist, spent nine months in Syria for this mission, capturing moments on camera and film for historical documentation and intelligence purposes.

“Seeing the National Guard, regular active, and Army reserves, all firing full cylinders was really cool throughout the operational area,” Sgt. Hernandez said.

For him, the deployment provided a valuable opportunity to see the Army’s impact up close and personal, while contributing to the operational mission.

“We capture the moments that are necessary for the world to see. We try to capture the Army in its best essence every single time we’re out there, [showing] all the different kinds of units that the Army provides,” said Hernandez.

The outstanding work of the 55th Signal Company will continue to serve as the “Eyes of the Army,” documenting the experiences and efforts of Soldiers all over the world. In the words of Staff Sgt. Nieves, “We remain available whenever they need any Soldiers for missions; we’re here and ready to go.”

Chaplain Col Paul R. Jaedicke on the Five Stages of Grief

Everyone suffers significant losses and reversals, such as a breakup or divorce, an illness or an injury, a loss of rank or reputation, failure at school or work, or the death of a family member or friend. When such losses occur, it’s important to remember that while your life has forever changed, a healthy grief reaction will ensure you won’t always feel the way you do at the time of the loss. For healing to occur after a loss, it’s important to go through all five stages of grief. The five stages of grief are typically labeled Denial, Anger, Guilt, Genuine Grief, and Resolution.

Denial is when the person suffering the loss momentarily refuses to believe the loss is really happening to him or her. This stage usually does not last very long.

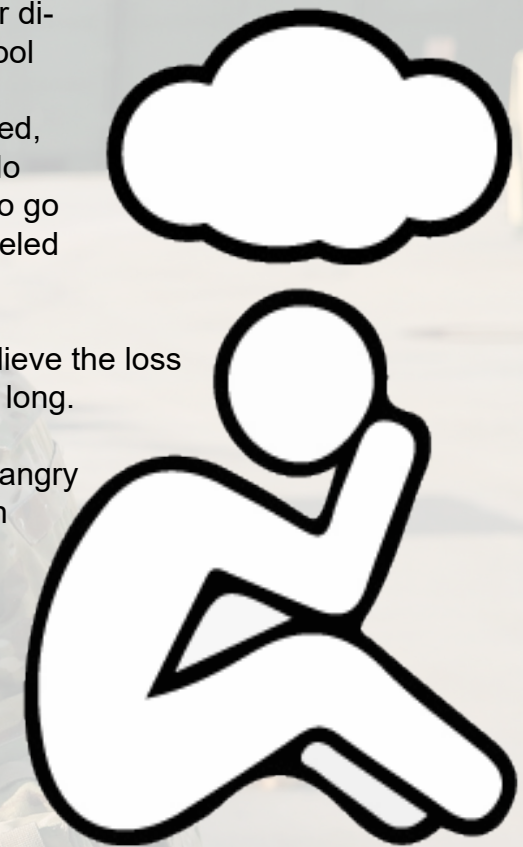
The Anger stage is when the person suffering the loss experiences an angry reaction toward someone other than themselves. For example, we can be angry toward the person who died, even though the deceased person may not have been at fault. Young children who lose a parent due to divorce or death will experience anger toward their parents. Many people become angry at God for allowing the loss to occur. These are all normal reactions to relatively abnormal events involving significant loss. In order to move through the anger stage, it is important for those who suffer loss to forgive those with whom they are angry.

The third stage of grief is Guilt. In this stage, grieving people become angry with themselves and begin to feel guilty about their own “mistakes” which may have contributed to their loss. Sometimes, grieving people blame themselves for their loss and then punish themselves with self-critical thoughts. During this stage, it is important to remember that hindsight is always better than foresight. If it’s necessary, it’s also important for grieving people to forgive themselves in working through any guilty they may feel.

Stage four is Genuine Grief which is weeping or a good cry. This is perhaps the most important stage and extremely necessary. The outpouring of emotion, whether done in public or private, provides much needed relief.

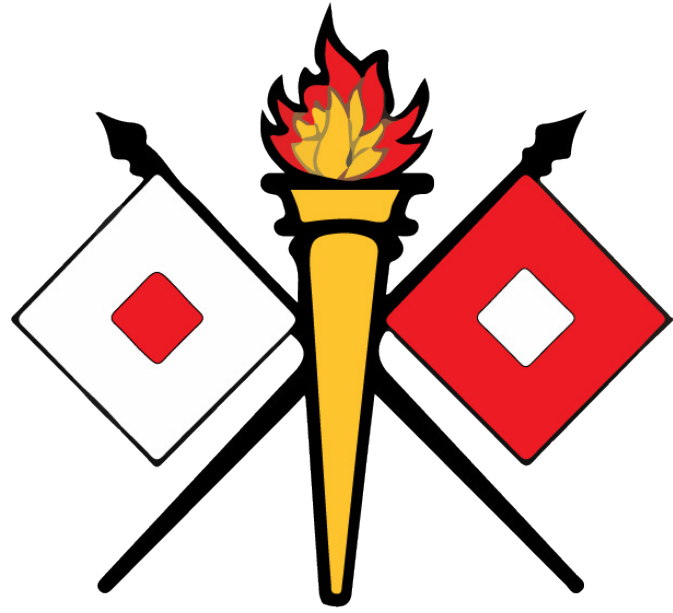
The last stage of grief is Resolution which happens automatically after the first four stages are complete. In this stage, a grieving person regains his or her zest and joy for life.

While some people go through the five stages of grief more quickly than others, the nature and significance of the loss will impact the time it takes to complete the grieving process. The key is to move through all five stages without getting stuck. When you or someone you know suffers loss, it’s good to remember that grief often lasts longer than your friends expect it to and is stronger than they can appreciate. When such losses occur, while your life has forever changed, a healthy grief reaction will insure you won’t always feel the way you do at the time of the loss.



History of the Mercury

<https://signalcorps.org/>



The association between the Roman god Mercury and the United States Army Signal Corps can be traced back to the historical and symbolic significance of Mercury as a messenger and communicator.

Mercury, known as the Roman equivalent of the Greek god Hermes, was considered the swift messenger of the gods in ancient mythology. He was known for his speed, agility, and ability to travel between realms, making him the ideal deity to deliver messages.

The United States Army Signal Corps is responsible for providing communication and information systems support to the U.S. military. Its primary mission is to ensure reliable and secure communication channels for the Army. The Signal Corps plays a crucial role in transmitting messages, coordinating operations, and providing vital information to military units.

The choice of Mercury as a symbolic figure for the Signal Corps reflects the importance of swift and efficient communication within the military. The association implies that the Signal Corps, like the god Mercury, acts as a messenger, facilitating the transmission of information and ensuring the smooth operation of military communications.

Furthermore, Mercury's depiction with winged sandals and a caduceus (a staff with entwined serpents) also aligns with the symbolism of the Signal Corps. The winged sandals symbolize speed and mobility,

characteristics essential for military communications. The caduceus represents the staff of Hermes/Mercury and has become a symbol associated with medical services. In the context of the Signal Corps, it may symbolize the role of communication in coordinating medical support and services on the battlefield.

Overall, the association between the god Mercury and the United States Army Signal Corps underscores the importance of efficient and reliable communication within the military, highlighting the role of the Signal Corps in delivering vital messages and information.

Continued from CSM McCoy...

our team and how we operate as an organization. I challenge you to look around your footprint and identify where we could improve. How can we better transform our professions, best practices, and operating procedures to maintain relevancy in the 21st Century? These are conversations we must have with ourselves. We owe it to the team to not only do the right things, but to also do things the right way.

This is NETCOM!! We set the standard.



B/392nd ESC Expands Theater Signal Assets

- By Candy Knight, 2d Theater Signal Brigade

Members of the 392nd Expeditionary Signal Battalion's Bravo Company set foot back on American soil in April following their Regionally Aligned Forces rotation to Europe, where the team worked to expand U.S. Army Europe and Africa's signal assets. By providing reliable and secure Internet connectivity and communication assets, the team enhanced the 2d Theater Signal Brigade's ability to deliver interoperable theater communications and cyber capabilities in support of combat forces and mission partners in Europe and Africa.

"Bravo Company's primary responsibility was providing access to the Department of the Defense Information Network and USA-REUR-AF's Mission Partner Environment, while maintaining a high quality of Internet protocol router network access to our supported units," said Capt. Mackenzie Ethan Moore, Company Commander. "To accomplish this level of support, we operated and supported several communication nodes spread across the European region."

Compromised of Army Reserve Soldiers, B/392d resolved multiple complex electronic and mechanical maintenance faults. The operations team coordinated daily sus-

tainment activities with numerous sustainment pushes each week. The Network Operations team coordinated with Battalion NetOps, Regional Hub Node, and the USA-REUR-AF's Mission partner Environment teams to remedy various technical issues.

"By deploying Soldiers who bring real-world IT experience, we can provide a diverse set of talents that increase the technical capability of the 2d Theater Signal Bde," Moore said. "At one point, we had a significant portion of our team deployed across the theater, located in multiple countries, supporting several active missions. In addition, we supplemented both 44th organic Scalable Network Nodes and Battalion Network Operations teams."

Despite becoming a full company only three months before mobilization, the B/392 met one of the highest Signal Company RAF deployments in recent memory.

"We were able to do so all because of the skills, personalities, and experience our Citizen Soldiers bring," Moore said. "They performed as any unit could, and they will return to their families, communities and jobs knowing they performed to the best of their

abilities, and gave more than the Army asked of them."

Moore stated that one of the most valuable experiences for his team was getting to work with Soldiers from other branches of the service and other countries.

"Being a part of the only Expeditionary Signal organization in Theater, our ability to provide enduring mission support allows USAREUR-AF to increase its capacity to support exercises and real-world events," he said. "Providing signal support for the Mission Partner Environment has been indispensable for multiple assure and deter missions across Eastern Europe. Ensuring our NATO allies can communicate and share data to make better-informed decisions has been one of the most rewarding aspects of our time out here."

Visiting parts of Europe during their rotation provided many memorable experiences.

"We enjoyed the tour to Europe," Moore said. "Arriving several months into the Ukrainian War and being a part of what the U.S. and its allies are doing to build readiness and interoperability has been tremendously rewarding and

Continued from Data-Driven...

in ARCYBER's G3.

Working with SEI, DSC-Pittsburgh produced a tool to detect the presence of malware beacons based on network traffic data. This tool was trained on synthetic data and tested during the Gaining Cyber Dominance exercise in Pittsburgh.

Data-Driven Decision Making is a key factor in continuously improving and modernizing, and NETCOM is uniquely poised to utilize network data. DSD remains on-call to advise and assist on with any data challenges. Feel free to reach out!

Continued from What Does a G-5...

endpoint for security compliance, 3) automatically remediate deficient endpoints, 4) authorize compliant endpoints, and 5) enforce policy and report results. C2C ensures endpoints continuously remain in accordance with standards by managing access to the network and its information resources, restricting access for those devices that do not adhere to established criteria.

Internet Protocol Version 6 (IPv6)- In coordination with Army Cyber Command (ARCYBER), G5 is providing input for the proposed architecture and addressing scheme for the IPv6 Limited Deployment Expansion (LDE) effort. The Army's intent is to provide all DoD, a data-centric approach as an option, to simplify automation of IPv6 and incident response.

Currently in testing, it will standardize routing, security, and cloud policies, provide richer context per flow for DCO analysis, make it easier to teach, learn, manage, troubleshoot, hunt, and interoperate with no additional cost, and mirror production networks in labs for continuous real-world evaluations, and red teaming. Once testing is completed, it will be submitted for approval and ARCYBER/NETCOM will then move into HQDA Phase 2 - Authority to Operate (ATO) & Change Requests Approvals.

Software Defined Wide Area Network (SD-WAN)- NETCOM G5 is working the SD-WAN technology within the DoDIN-A. The Army will leverage SD-WAN with additional security components to transi-

tion off JRSS gateways and optimize Army traffic routing and access with the DoD divesting of the Joint Information Environment (JIE) and shifting to a Zero Trust Architecture (ZTA). The shift in Software Defined Networking (SDN) and Network Function Virtualization (NFV) technology increases the Army's operational efficiency by centralizing network management through orchestration.

Army Futures Command (AFC) Information Technology as-a-Service- The Army Futures Command (AFC) Information Technology as-a-Service Initiative includes Multi-Domain Operations (MDO) standardizing capability-based modernization that merges Integrated Enterprise Network and Integrated Tactical Network (IEN/ITN). This effort also includes Army Unified Network Plan (AUNP) management, integration of capabilities through collaboration with stakeholder organizations, and supporting Army Futures Command (AFC) IT services oversight and the development of future acquisition contract initiatives.

So who do we talk to about the future of the Army networks and the role NETCOM has in this vision? We need only to go to the NETCOM G5.

Continued from CG..

will be responsible for synchronizing cybersecurity and network efforts across the globe in support of the Army. There is a lot of work still to be done, but I am sure of one thing, this team can get it done on all fronts.

Finally, I want to personally thank every team member for what you have done and what you will do in support of the Army Unified Network. I am proud to be a part of this team and proud of what we do for the Army every day.

NETCOM...Enabling Decision Dominance!

MG Christopher L. Eubank
Commanding, NETCOM



Regional Cyber Center - Korea

Possibilities - Being All You Can Be

- By Maj Ray Blockmon, Regional Cyber Center - Korea

In the past year, the RCC-K team participated in several training events. In April, the Sergeant Major, the Systems Management Branch OIC, and members from the Defensive Cyberspace Operations Division, participated in the Capture the Flag (CTF) event that was hosted at TechNet, Honolulu, Hawaii. The event tested each participant on different methods of offensive cyber and hacking capabilities. Events such as extracting credentials from Wireshark packet logs, deciphering Secured Socket Layer (SSL) connections, and understanding what the threat actor attempted, or achieved to do in their exploitation were presented to the teams to negotiate. Fundamentally, CTF challenged every member on the RCC-K team and required that each member worked together to piece together clues to solve each event.

Training is a fundamental requirement that ensures the RCC-K maintains the technical expertise in all enterprise systems that it employs and manage.

Over the past year, the team participated in numerous training events. For example, this past June, the Network Management Branch (NMB) team, sent two members to Las Vegas, Nevada, to participate in the Cisco Live event. The week-long training event allowed participants to attend several different seminars that aligned to their profession. Completion of the seminars provided the participants with Continuing Education (CE) credits, which are used to renew Cisco certifications every three years. The RCC-K has scheduled more personnel to participate in June 2023 Cisco Live event.

In April 2023, the RCC-K sent several members to participate in the Certified Information Systems

Security Professional (CISSP) two-week class. This allowed individuals who have spent months of rigorous training and study to tie it all together and attempt the certification. The length of the grueling exam is four hours with questions ranging from 125 to 175 – depending on how well (or bad) during the exam. It spans from eight domains, such as Asset Security to Software Development Security. The class was delivered in a classroom environment at the Camp Humphreys' Comms Center. Additionally, other certification exams have occurred at Camp Humphreys that our RCC-K team have been able to attend such as CompTIA Security+.

As the RCC-K continues to improve the enterprise, other training requirements have been provided to maintain relevancy with emergent technologies. Security appliances, sensors, and endpoint management capabilities such as ForeScout, NetScout and Microsoft Intune have either been fully adopted or are in development within the Korea Theater of Operations (KTO).

One of the most significant challenges that our workforce face, is the ever changing and adoption of technology. As new requirements are determined to support the commander, this forces the team to become flexible in their career field and with their current skill set. No longer can we remain comfortable; we adapt, seek every learning opportunity available, and persevere through continuous changes in the fluid KTO environment. To support the customer base, this requires the RCC-K to stay on top of our game and take advantage when training opportunities are presented.

Army Life

Quality of Life Improvements for Soldiers and Civilians, Programs, Services, and Events)

- By Maj Ray Blockmon, Regional Cyber Center - Korea

With our new administrative relationship with 1st Signal Brigade this year being fruitful, many benefits have immediately materialized. Our move to Camp Humphreys has been extremely beneficial to our enlisted Soldiers and our Department of the Army Civilians (DACs). Training opportunities, increased exposure to the Korean culture in Seoul, and access to Incheon International Airport being only two hours away, enhanced the quality of life and wellbeing of our organization.

Our ADCON partnership with the 1st Signal Brigade significantly simplified executing RCC-K support requirements, of which many materialized immediately. Additionally, the response time for administrative actions that includes awards, promotions, and retirement actions are processed in a timelier manner. Lastly, our move to Camp Humphreys enhanced the quality of life and wellbeing of our organization with more training opportunities, increased exposure to the Korean culture. Programs such as the Better Opportunity for Single Soldiers (BOSS) and the Morale, Welfare and Recreation offer increased support capabilities at Camp Humphreys.

The RCC-K's enlisted Soldiers are presented with many opportunities for participation. For example, the Best Warrior Competition and to compete for the Expert Soldier Badge (ESB) which are hosted by the

2nd Infantry Division. These training events are critical for our Soldiers' professional development because they offer promotion points, provide invaluable leadership training, and support esprit de corps.

Both Soldiers and DACs also participate in training that aligns to their DODI 8570 Information Assurance baseline certification requirements. (ISC)2's Certified Information Systems Security Professional (CISSP) and CompTIA's Security+ training are hosted often, allowing the RCC-K workforce to remain current with their conditions of employment.

Members of the RCC-K who have brought their dependents have access to an expanded housing market. It also includes a large Department of Defense Education Activity (DODEA) footprint, consisting of two elementary schools, one middle school and one high school. After school activities for children are plentiful, offering families a safe and friendly environment to enjoy. The transition to Camp Humphreys has truly been a blessing for the RCC-K. The organization is excited for the next chapter in our support for the peninsula and eager to team with the local community to foster a bright and enduring relationship.

Data Based Decision Making: Supporting a "People First" Priority

- By MAJ Donald F. Ingham, USASA Camp Roberts - Commander

The following article is based on a fictional scenario:

It was getting late. The accountability battle drill, recently practiced over 12 times, had just been initiated; this time, it was in response to a real-world situation. In the last 8 hours, an unprecedented amount of rain drenched the local area, extensively flooded roadways, necessitated mandatory evacuations, and resulted in at least one casualty. 20 Soldiers working 12-hour shifts knew the Company couldn't send everyone home. The United States Army Signal Activity (USASA) – Camp Roberts mission to provide Information Networks and Services to everyone from President to Private, was too important. But can the incoming shift make it to site? If they can, will on-site personnel be able to make it home? Are family members safe?

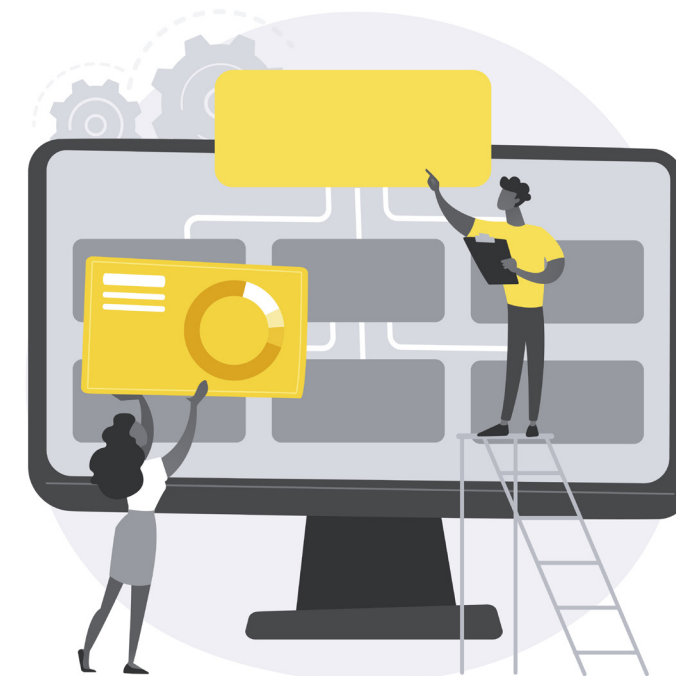
The Command team had to quickly account for 109 Soldiers and 62 Department of the Army Civilians, living up to 75 miles apart, during a natural disaster. Accountability would likely take up to an hour, while everyone was waiting for a decision to be made on whether to execute shift change or go into lock down. This decision needed to account for the risks presented by evacuations, road closures, and sleep deprivation. With 12 vehicle accidents in the previous year, safety was at the forefront of everyone's mind. Who can safely make it to site? Who needs to leave site immediately to help evacuate their family? Fortunately, the USASA – Camp Roberts team was proficient in data-based decision making.

The command team knew they had an extensive amount of Soldier data, and immediately got to work. A software application called Microsoft Power BI, which is accessible on government computers, facilitates the visualization of data, and streamlines the process of turning data into information. This tool gave leaders an ability to quickly plot addresses on a single interactive map, which allowed leaders to drill into flood zones and quickly identify several problems. One Soldier lived in

an evacuation zone and needed to leave work ASAP to assist his pregnant spouse. A second (off-shift) Soldier was surrounded by water and shouldn't leave his home at all. 34 more Soldiers lived in an area that was likely inaccessible. So, shift change or lock down? The command team needed more information.

Fortunately, Power BI was able to drill even further to correlate each Service Member by shift. This allowed the team to understand that there were enough available personnel, excluding the people identified as residing in high-risk areas, to execute the operational mission without going below minimal manning. The weather forecast offered the last pertinent data point – there would be a temporary window of opportunity at 1800 – an hour earlier than typical shift change. Should the team execute shift change, or lock down?

Within 30 minutes (notably before 100% accountability had been achieved) the team had all the relevant information to make an educated decision. The analysis brought to light a potential third course of action



304th ESB-E Continues on the Path of Modernization

- By Sgt. Noah Sladek, 1st Signal Brigade

After completing their conversion in July of 2021, 304th Expeditionary Signal Battalion (ESB) became Enhanced (ESB-E), modernizing itself to the military's new methods of tactical communication. The storied battalion, with over 100 years of service, now has the capabilities to transport quicker, equip faster, and maneuver across the battlefield like never before.

The Army has been pushing itself to re-configure the mobility of tactical communications by fielding multiple ESB units with new and enhanced capabilities. With the new capabilities of the equipment, mainly being the new network node that is included, units are finding their transportation requirements significantly reduced, including 304th ESB-E. Before the switch to enhanced equipment, the main source of communications came from legacy network nodes and Satcom Terminals, which have been completely done away with here. Not having to haul, pull, and maneuver larger communication equipment has been the key to modernizing the unit.

"The ability to deploy rapidly with smaller equipment that does not take as much logistics is really beneficial in this environment," said Chief Warrant Officer 2 Ashton Warrington, the Senior Network Technician at 304th ESB-E, 1st Signal Brigade. "We don't have to worry about sling loading, we don't have to worry about as much logistical work it would take if we were using humvees and trailers, it is a lot easier to deploy with it"

As an Expeditionary Signal Battalion on the Korean Peninsula, 304th ESB-E must be able to support virtually all units, which include the United Nations Command, Combined Forces Command, United States Forces Korea, and Eighth Army. They were the third battalion to be converted under the plan



Soldiers from Bravo Company, 304th Expeditionary Signal Battalion-Enhanced assemble the new enhanced equipment in the Republic of Korea, on Jan. 18, 2023. (U.S. Army photo by Sgt. Alex Estrada / 1st Signal Brigade)

to modernize several brigades with the Capability Set 21 fielding equipment. As the Army aims to keep on track with its modernization process, it will soon unveil additional enhanced capabilities over the next several fiscal years.

Another huge benefit to the current enhancements is the ability to use commercial net-

works to operate. There are signal units now using Starlink, which is operated by SpaceX, and helps speed up communications faster than previous equipment.

"The biggest differences with current enhancements that we did not have with the legacy equipment at the time is the ability to use commercial assets," said Warrington. "You could not use a Wi-Fi or any commercial asset like that to establish communications, but we have that capability now because it comes with the devices we use today."

From a Soldier's perspective, all of these new devices are made to make their job simpler, and easy to move with. The applications being put in place make learning the new processes straightforward, and more accessible for commanders.

The Army's IT Professional of the Future

How Soft Skills will Complement Hard Skills Enabling Multi-Domain Operations

- By Dr. James E. Cronkhite, 106th SIG BDE Civilian Executive Officer

General James McConville, 40th Chief of Staff, Army, noted in The Army People Strategy (2019). "Winning matters, and People are my number one priority. People are our Soldiers – Regular Army, National Guard and Reserve - their Families, Civilians, and Soldiers for Life – Retirees and Veterans. We win through our people, and people will drive success in our Readiness, Modernization and Reform priorities. We must take care of our people...". The U.S. Secretary of the Army, the Honorable Christine Wormuth, reinforced the focus on personnel development and training in the Army Digital Transformation Strategy (2021). Furthermore, the Army Data Plan (2022) emphasized people and culture as critical stepping-stones to success in a multi-domain environment. Given the Service-wide operational transition from IT-centric applications and skill sets to data as an artifact which enables users to find, access, understand, employ, link, and protect data; then it naturally follows that training and education for the IT workforce must blend the traditional focus on technical characteristics with non-technical attributes such as creativity, critical thinking, adaptability, and a willingness to learn and maneuver through an ever-changing landscape.

Soft Skills in an Organizational Setting

Traditionally, training and education focus within the IT community was centered on what would be considered hard skills. Hard skills are normally those specific capabilities, abilities, and skill sets that employees possess and demonstrated in a measured way. These learnable skills then enable

the employee to perform job-specific tasks such as troubleshooting desktop PC or laptop operating systems failures or programming routers for LAN/WAN interconnectivity.

In contrast, soft skills, also known as people skills, are a mixture of interpersonal, social skills, and character traits that include critical thinking, teamwork, creativity, and communication skills.

Soft Skills and the Army IT Professional

Within the IT community, soft skills play a critical role in providing improved interpersonal communications and customer service and the ability to adapt to changing technology and technological requirements. As an Army IT employee, the ability to communicate with colleagues, supervisors, and customers can be harnessed to help resolve IT issues and embrace the power of technical tools and analytics. Nearly all IT disciplines and workplace

environments require substantial communications skills whether it be manifested in the ability to brief senior leaders or non-technical personnel on technical issues, drafting proposals or inter-office communications, or providing instruction to non-technical personnel on

the use and applications of IT resources.

Furthermore, critical thinking and creativity enable more rapid troubleshooting methods while anticipating future challenges and developing solutions to said challenges. Critical thinking entails interpreting,

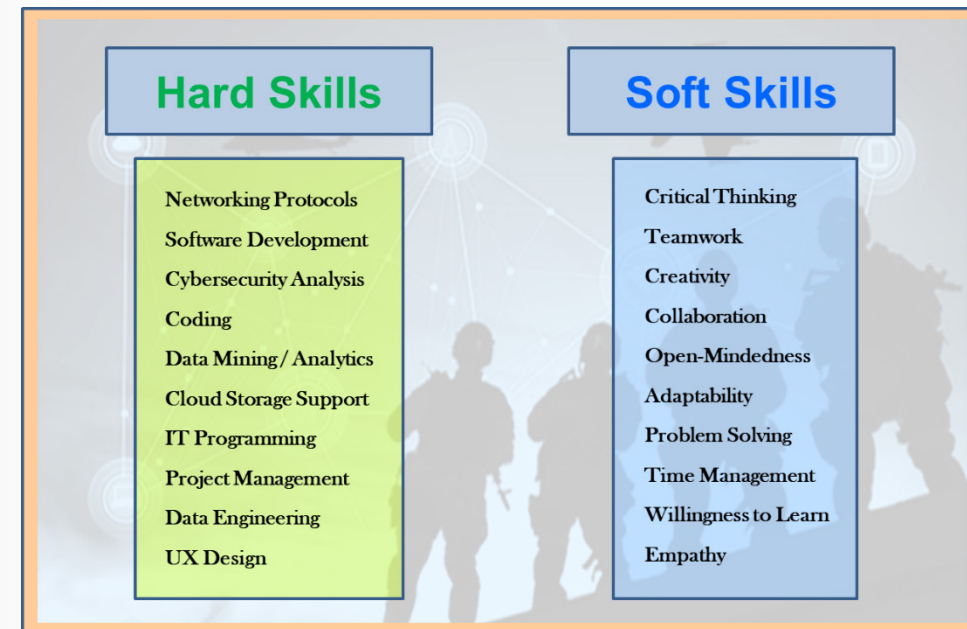


Figure 1. Hard Skills vs. Soft Skills

Continued from B/392nd ESC...

meaningful. Spending nine months in Poland, we experienced first-hand the country's rich culture, and wonderful sense of duty."

The future is bright for the B/392d, according to Moore. The experiences he and his team gained during their European rotation gave them vital training opportunities on new equipment in an operational environment.

"The B/392d will convert from an Expeditionary Signal Battalion to an Expeditionary Signal Battalion – Enhanced," he said. "This rotation is an excellent example of the Army's active-duty component providing mutual support and training to the Reserve component."

Continued from Data Based Decision...

– conduct shift change at 1800, exclude the vulnerable population, and get our affected personnel home ASAP. This teams ability to speedily turn data into information allowed them an ability to use a metaphorical decision scalpel instead of a hammer and potentially avoid a dangerous situation. This decision resulted in no degradation to the operational mission and no vehicle accidents.

Leaders must make the best decisions they can with the information at hand. The beauty of a data visualization tool like Power BI is that it allows front-line leaders to aggregate and combine data from the multitude of different military datasets for their unique purposes. Want to write an ACFT incentive policy? Combine DTMS score data with IPPS-A personnel and leave data to automatically determine who should be in formation each day. Add MED-PROs into the mix to streamline Leave approval. The untapped potential of operationalizing data literacy is immense. If executed properly, visualizations work in conjunction with front line leaders to create a culture of "data-driven, yet Soldier centric" leadership. It is important to note that these capabilities do not replace face-to-face interactions, instead they allow leaders the time to create more meaningful relationships. With easily accessible information, organizations can manage more efficiently, which gives leaders time to execute true leadership. USASA Camp Roberts is fortunate to have fostered this data-driven culture, which begins immediately

as Soldiers in-process. One of the first things a new Soldier does is fill data into a "mass tracker." Sections routinely maintain individual data that cannot be pulled from a system of record (for example, what shift someone is on, if they have a civilian drivers license, etc.). This is automatically combined with datasets from MedPros, IPPS-A, DTMS, UCFR and more to automatically provide leaders with a baseline for daily decision making and an accurate/accessible dataset for quick use when emergencies arise.

Necessity is the mother of all innovation. Whether it is an unexpected torrential downpour threatening a strategic satellite instillation or Large-Scale Contingency Operations, the future demands that the US Army is able to quickly turn data into information. Furthermore, the future is unknowable. It is likely impossible to standardize a one-size-fits-all company level dashboard that can meet the rapidly changing needs of a dynamic battlefield. What is possible is an investment in people. Training data literacy (preferably at the BOLC level, at minimum) will ensure that front line leaders have the skills they need to enhance their units, take care of their people, and continue to get the message through.

Continued from Regional Cyber...

In the RCC-K, not only do we support and execute the operation and maintain (O&M) mission, but we also lean forward to engineer and install (E&I) solutions for the peninsula when required – and relish this challenge. The training that we receive, and the collaboration and coordination efforts made between our professionals is what allows the RCC-K to support the KTO – to include manning and defending the Mission Partner Environment.



1st Cyber Battalion Soldiers Give Back Through Volunteer Work in Local Community

- By Shatara Riis, Cyber Protection Brigade Public Affairs

The 1st Cyber Battalion "Legendary Defender" Soldiers seek opportunities to serve outside of the Army and within the local community. That helping hand comes through working with Greenbrier Middle School in Evans, Georgia, and serving at an Augusta-area animal shelter. "Over the last several years, members of the 1st Cyber Battalion warrant officer community have volunteered more than 200 hours to enrich Greenbrier Middle School's curriculum and train students in cyber security in support of CyberPatriot," said Capt. Eva Sung, Headquarters & Company A, 1st Cyber Battalion, commander. According to its website, CyberPatriot is the National Youth Cyber Education Program created by the Air & Space Forces Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering and mathematics (STEM) disciplines critical to the nation's future.



"We hope that having Soldiers help educate and mentor young people in cybersecurity will help cultivate their interests and spark curiosity to pursue further education on the topic," Sung said.

Continued from Warrant Officer...

solver, trainer, and mentor are traits that positively influence the NETCOM and Army culture, and are traits we must always pass on to our teammates; it's those future leaders who will be influenced by what we teach them today. Always remember, we are on audition every time we are in public.

Lastly, at NETCOM, warrant officers play a critical role in achieving the Commanding General's LOE 3 – "Continuous Improvement". Part of Continuous Improvement is to achieve a Unified Network

"Cybersecurity is consistently increasing in complexity and evolving as technology continues to advance. Those young students will be the future of the cybersecurity profession."

Some of the Legendary Defender Soldiers walk and play with dogs at an Augusta-area animal shelter to give back.

"(Volunteering) is an excellent opportunity to give back to the communities within the Augusta area and integrate Soldiers into their local communities to help build the military and civilian relationships here in the CSRA," Sung said.

The CSRA is the Central Savannah River Area, serving a 13-county region in the eastern portion of central Georgia. While the Legendary Defenders currently assist Greenbrier Middle School, the battalion seeks to extend its support to Greenbrier High School, as a part of Fort Gordon's community outreach program, known as "Adopt A School."

"We recently partnered with Greenbrier High school to develop our relationship with them," Sung said. "We look forward to conducting events in support of the high school over the summer and into the new school year."

on the DoDIN-A while adhering to Zero Trust Principles. There are challenges to achieve these efforts, so we as warrant officers, must bring our technical expertise to get after these operational and strategic requirements. There is a reason only the very best is selected to become part of the cohort. We are technical experts, trainers, and advisors, and our commands and Soldiers deserve the best the cohort has to offer. We must have a positive impact on NETCOM today and in the future!



Spc. Alexander Fabian assembles part of the new enhanced equipment set in the Republic of Korea, on Jan. 18, 2023. (U.S. Army photo by Sgt. Alex Estrada / 1st Signal Brigade)

As the Army continues the momentum on modernizing necessary equipment, it is safe to say the new technologies being fielded are helping in everyday operations.

“With all the experience I have had with the equipment, the SNN has been very simple to use, you can log right in and make any adjustments you need, and the setup is what makes it very easy and accessible,” said Spc. Jamarious Battle, Nodal Network System Operator for Charlie Company, 304th ESB-E.

304th ESB-E is one of many units being an example of the innovations being done to support these plans.



Soldiers from Bravo Company, 304th Expeditionary Signal Battalion-Enhanced work together to put up the new enhanced equipment set in the Republic of Korea, on Jan. 18, 2023.

Brigade Hiring Fairs Address Recruiting and Retention Challenges

- By Tracy B. Lyng, 7th SIG CMD, Strategic Communications Officer

To address the challenge of recruiting and retaining Civilian IT professionals, 7th Signal Command’s 93d and 106th Signal Brigades hosted virtual hiring fairs during the past year that proved wildly successful at identifying and bringing on board talented candidates in fields including information technology, cyber security, logistics, and management support.

Since January 2021, the 93d SB had lost an average of 0.5% staffing per month, with net losses for 16 of the previous 20 months. Its staffing percentage dropped below 90% in November 2022 for the first time in over 4 years. To counter this trend, the 93d Signal Brigade planned a virtual hiring fair for 1-2 December 2022, in consultation with Army Cyber Command and the 7th Signal Command (Theater).

The brigade set aggressive performance targets to increase staffing by 10%, which equates to a net gain of 114 personnel. Accounting for internal hires, expected losses in Dec through Feb, and declinations, this equated to 250+ hiring actions.



Pictured: Mr. Steve Brown (Dep CDR 93d), Mr. Andre’ Wiley (Mid-Atlantic Dir), Ms. Alice Goodson (Central Dir), Ms. Geeta Watts(93d S1), Mr. Terance Whitlock (Bluegrass Dir), Mr. Steve Giza (Southeast Dir), Mr. Rod Hutchinson (South Atlantic Dir), Mr. Van Jarrel (Gordon Dir)

Prior to the hiring fair, the brigade undertook a publicity campaign to solicit resumes from the public for consideration. On 1-2 December 2022, talent management directors, brigade senior leaders and managers, and human resources professionals came together at the South Atlantic Regional Network Enterprise Center, Fort Eustis, Virginia, to pilot streamlined recruiting processes, identify candidates, and extend offers for hard-to-fill positions.

During the two days of the fair, the brigade processed 267 recruiting actions, extended preliminary offers, and secured preliminary commitments. As a result, January onboard numbers reflected a net increase of 58 employees (5% staffing increase) bringing staffing to 93% of authorizations—the largest single increase in staffing for a single month since brigade was reactivated in 2009.

Overall, the brigade projects a net increase at or near 10% just as a result of this hiring fair, and all eight Network Enterprise Center directors who participated exceeded their performance targets for qualified candidates.

Based on the success at the 93d SB, the 106th Signal Brigade, headquartered at Fort Sam Houston, Texas, decided to hold their own virtual hiring fair, requesting resumes by 10 February and conduct-



Photos Courtesy of the 55th Combat Camera

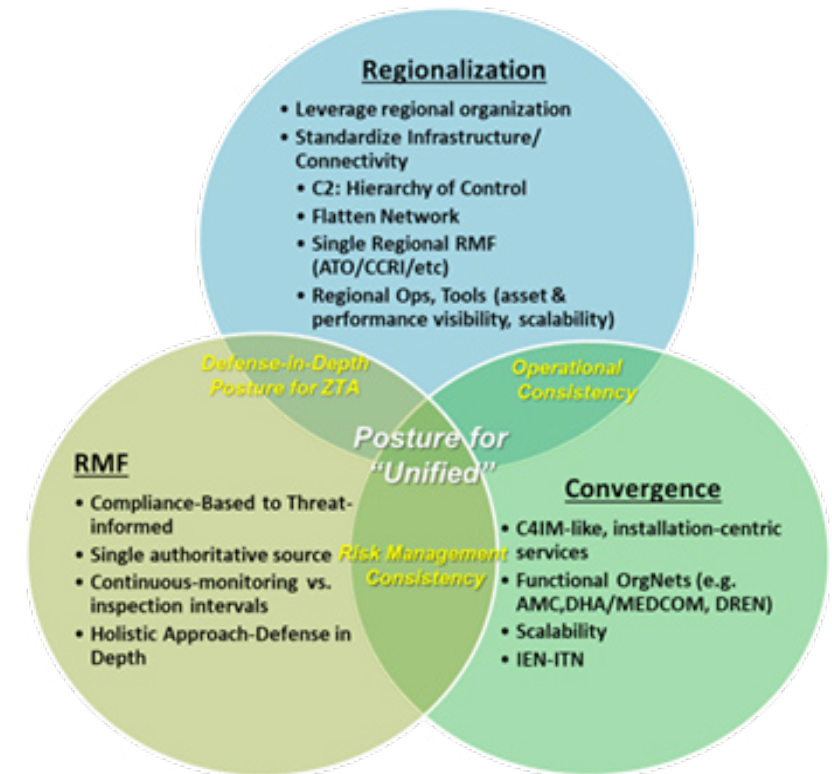
Posturing the CONUS Theater for Unified Network Operations

- By Tracy B. Lynge, 7th SIG CMD, Strategic Communications Officer

The 93d Signal Brigade, headquartered in Ft. Eustis, Virginia, is leading the way in setting the stage for the Unified Network. With support from higher headquarters, Col. Kristy Perry has pursued a three-pronged strategy within the 93d's area of operations that will posture the organization for 1) Army Unified Network Operations and the integration of the Integrated Enterprise and Tactical Networks; 2) the shift of the Risk Management Framework to focus on threat-informed risk management and operational readiness; and 3) installation and organizational network modernization and convergence.

Regionalization. First, the 93d is moving to ensuring standardization of network infrastructure and connectivity across all of its Network Enterprise Centers (NEC). This is the first step in enabling consistent, scalable command and control. This move will also support strategic objectives 6 through 9 in the Army Data Plan, as the brigade will be able to build a core capability to use data, analytics, and visualization to improve the quality and speed of decisions at every level to solve problems, predict outcomes, and prescribe performance level.

Risk Management Framework. The 93d is centralizing the process for preparing for inspections, placing that responsibility on regional Network Enterprise Centers (NEC) and allowing local NECs to focus on local activities. The team is also assessing cyber readiness from a "threat-informed" perspective to leverage the capabilities of continuous monitoring to identify and remediate vulnerabilities, and reducing "compliance" checks in favor of ensuring "readiness." Piloted within the Southeast Region, with support from 7th's Cybersecurity Division, Fort Stewart Regional NEC staff are assessing relevant RMF controls to determine which ones can be objectively satisfied with data from authoritative sources. If so, cyber and technical SMEs at the RNEC and BDE can leverage automation



to eliminate labor-intensive, redundant efforts that cannot be scaled to cover changing controls, more organizations, more/new systems, and do this more frequently, or "continuously."

Convergence. The 93d is supporting the Army's efforts to converge functional organizational networks (OrgNets) and installations under regionalized networks to leverage the network architecture and security framework to provide, at scale, consistently reliable and secure services to a greater population of users, organizations, and installations. With the collapse of the network, activities that once were performed by each installation can now be performed centrally at the regional level. In the case of enterprise capabilities, these tasks will be performed at the enterprise level for all. This achieves economies of scale that free our workforce to do other, more emergent tasks at the installation level.

To support all of these efforts, the 7th Signal Command (Theater) recently realigned several NECs among its three brigades. The National Capital Regional NEC (Fort Belvoir and subordinate Local

analyzing, or evaluating information, arguments, or experiences with a set of reflective attitudes, skills, and abilities to guide personal thoughts, beliefs, and actions. Marcus Aurelius noted in Meditations “Nothing has such power to broaden the mind as the ability to investigate systematically and truly all that comes under thy observation in life”. Moreover, creativity, combined with critical thinking, empowers the Army IT professional by anticipating future challenges and the ability to develop solutions while building teamwork and a collaborative environment. In this case, creativity becomes the ‘icing on the cake’ and helps round out the Army IT professional in a multi-domain environment.

To this end during the recent Brigade Virtual Hiring Fair, resume reviews and interview questions were included that focused on both hard and soft skills to identify and recruit employees beyond the traditional IT certi-

fication-heavy standard. For example, the Brigade Headquarters was filling a desktop support technician in the IMO section and the resume review included not only relevant technical skills, but also which candidates documented work experiences related to critical thinking, collaboration, and communication skills. We then extended this paradigm during the interview process and our questions not only focused on technical skills but also experiential and soft skills-related inquiries.

Finally, the world of the Army IT professional is constantly changing. The move from traditional data storage solutions to the cloud, use of artificial intelligence applications and machine learning to improve IT service delivery and management, coupled with the movement to Zero Trust and focus on securing data and not the network will require adaptability and a willingness to learn as a fundamental char-

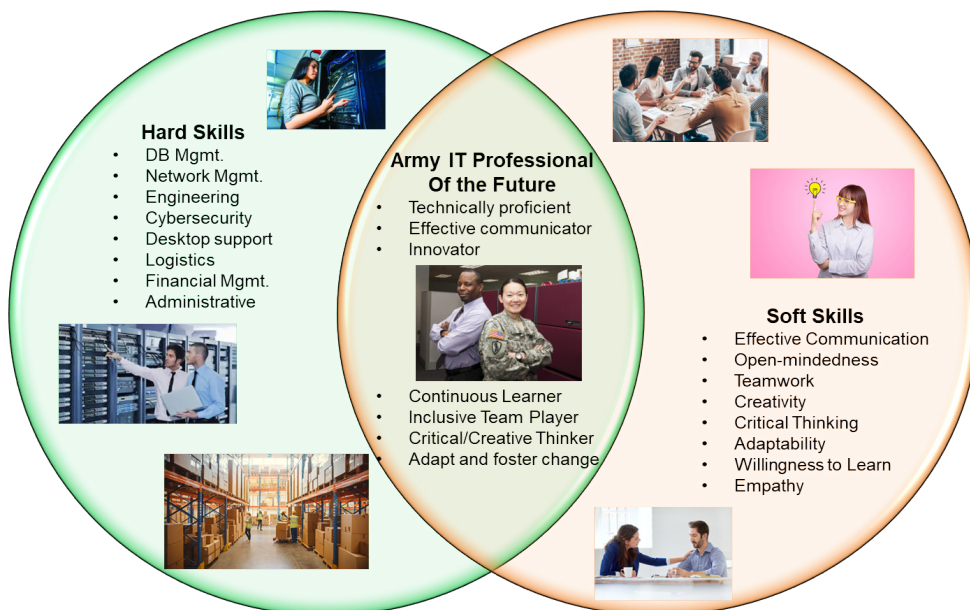


Figure 2 highlights the integration of hard and soft skills into the Army IT professional of the future

acter trait. The Army Data Plan noted: The right data, at the right time, at the right place will enable faster and better decisions at echelon – to out-think and out-pace any adversary. By its nature, the Army’s Multi-Domain Operations, as part of Joint All Domain Operations, has a larger and increasing scope than earlier military operations. Each domain has its own growing information and data flow, from open-source intelligence, space-based sensors, cyber-space queuing to Soldier medical status and vehicle self-diagnostics. Today’s Soldiers and Commanders require synthesis across these domains to dominate the battlespace. (Army Data Plan, 2022)

In conclusion, previous generations of IT professionals could count on hard skills and technical certifications as a means to succeed in the IT field. And this is not to say that hard skills and technical certifications are no longer required for the successful IT professional. However, the changing dynamics and rapid technological advances within the IT field challenges the Army IT professional to not only maintain current education and training standards but embrace opportunities for improving their respective soft skills. The Army’s People Strategy, the Army Digital Transformation Strategy, and the Army Data Plan all emphasize the changing nature of IT. Consequently, the Army must develop, nurture, and retain top talent in order to meet the geopolitical challenges in the 21st century. In doing so, leader engagement for soft skill training and development will allow the Army IT professional to truly shine and pave the way for delivering and managing IT services

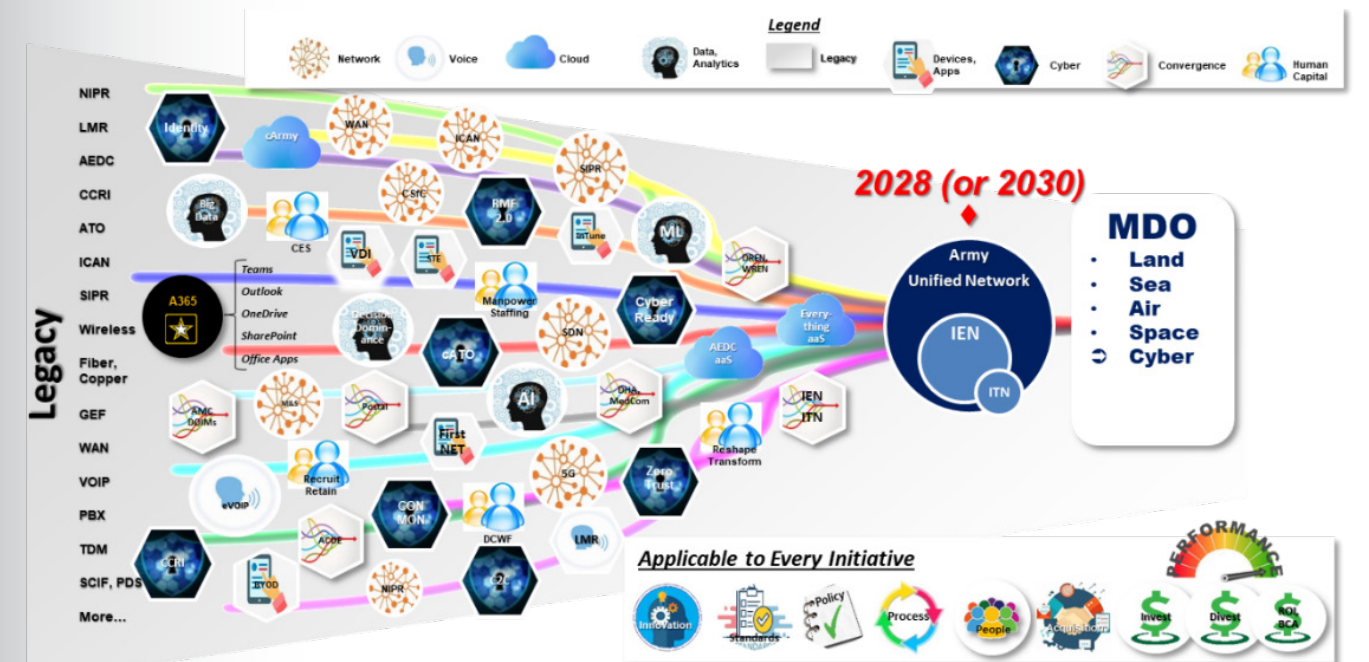
ing interviews 13 February to 2 March. This second iteration was just as successful as the first, with the 106th onboarding several personnel as a result, increasing their staffing.

The success of these hiring fairs exemplify the need for Army organizations to be innovative and aggressive in their recruiting efforts in today’s workforce environment.



NECs) moved from the 21st Signal Brigade to the 93d Signal Brigade; and the Central Regional NEC (Redstone Arsenal and subordinate Local NECs) moved from the 93d to the 106th Signal Brigade. This move better postures the 93d and the 106th for regionalization, the RMF shift, and organizational network convergence. It also allows the 21st to return its focus to its core SATCOM and national-level mission partner support missions.

The 7th Signal Command (Theater) and the 93d Signal Brigade will continue moving aggressively to support HQDA, Army Cyber, and NETCOM in modernizing and converging our network infrastructure to enable the Army Unified Network, a Multi-Domain Operations-ready force, and decision dominance.



106th Signal Brigade Leadership Profile

- By Tracy B. Lynge, 7th SIG CMD, Strategic Communications Officer

During the past year, the 106th Signal Brigade has welcomed new leadership. Brigade Commander, Col. Joseph N. Gardner, and Command Sergeant Major Wesley Stollings have a clear vision and ambitious plans for the brigade and its personnel.

The 106th, headquartered at Joint Base San Antonio, Texas, manages 19 Network Enterprise Centers that support Army and Joint Force installations and mission partners across 19 States from Florida to the Pacific Ocean—as well as 22 foreign countries. The brigade has over 1,300 Soldier, Civilian, and Contractor personnel; supports 170,000 Army personnel; and manages \$750 million worth of property and equipment.

When Col. Joseph Gardner assumed command in August 2022, he did not hesitate to declare his top priority. In his first remarks as brigade commander, Col. Gardner stated, “I welcome the challenge of ensuring every installation in this command’s footprint has the digital connectivity to serve as a power projection platform and command and control node for the Army.”

Nearly a year later, Col. Gardner says he has added two more priorities for his team for the upcoming year. “We want to standardize how we execute across the region—standardize the delivery of the network to our supported commands,” he stated. “And we want to synchronize initiatives at the NEC level, brigade level, and command level—if we do that, we can continue to do what we do best—enable, deploy, fight, win.”

Col. Gardner entered active duty in 1989, and received his commission as a Distinguished Military Graduate of the Army Officer Candidate School in 2001. Having served from the rank of private to colonel, Col. Gardner has this advice for young Soldiers—and Civilians—particularly those in the Signal and Cyber world.

“Becoming technically proficient is the most important thing,” said Col. Gardner. “You have to start by becoming an expert in your craft, so that someone will identify you as an individual with potential—someone they can mentor and advocate for.”



L-R CSM Sean Gerner, Col. Joseph Gardner, CSM Wesley Stollings (Photo Credit: Kara Carrier)

When asked about his leadership philosophy, Col. Gardner stresses the importance of authenticity and building trust. “Being candid and authentic with your team helps build trust, especially across a geographically dispersed organization like ours. If you are not authentic, people see right through that. And when trust is lost, the work environment becomes contentious, not just for the personnel involved in that relationship but for the entire organization. I always keep that in mind when interacting with my team.”

The 106th also welcomed a new command sergeant major during the past year. Command Sgt. Maj. Wesley Stollings assumed responsibility in February 2023, and he shares Col. Gardner’s vision of a brigade where all units are synchronized and standardized. “Individuals and teams



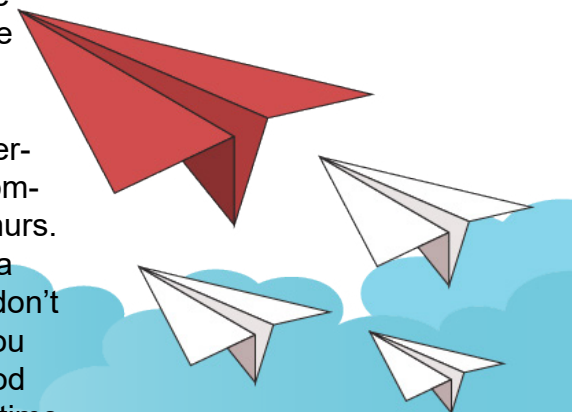
L-R Col. Joseph Gardner, CSM Wesley Stollings, CSM Sean Gerner (Photo Credit: U.S. Army)

may all be rowing—all in a good direction—but if Col. Gardner’s top priority and their top priority aren’t the same, there is a disconnect there,” he remarked.

Command Sgt. Maj. Stollings is focusing on recruitment and retention during the next year, as that is a top priority for the U.S. Army. He has asked all the non-commissioned officers in the brigade to “tell their story” within their communities, on social media, and in personal interactions. “I ask them to talk about their successes and what it means to them to serve in the Army,” he added, explaining that most Americans don’t have any connection to military service, so openly sharing their experiences can make a big difference.

Command Sgt. Maj. Stollings also wants to focus on the brigade’s mission and building up the team over the next year. “My goal is to let everyone here—Civilians as well as Soldiers—know that as the top enlisted personnel I don’t just advise the commander on military-related matters, and that they can come to me with any issue or concern,” he said.

When asked if he has a leadership philosophy, however, Command Sgt. Maj. Stollings demurs. “I don’t know if I would call it a philosophy, but I think if you don’t take yourself too seriously, you are loyal, and you have a good work ethic, 99 percent of the time you will be successful. Those are the values I try to embody.”



A special thank you to all of our Unit Public Affairs Officers (PAOs), Unit PA Representatives (UPARs), and NETCOM team members, who continue to support our efforts to tell the NETCOM story. We may all be in different states, regions, areas, but we are ALL NETCOM. What you all do matters, and we cannot succeed without a total team effort. We are always listening for ways to improve and look forward to any ideas you have. We are a success here at the NETCOM HQ PAO because of your input.



**MAJ Raymond Blockmon
Andrew Bosewell
Colin Broadstone
Dr. James Cronkhite
MAJ Kevin Goulding
MAJ Donald Ingham
Candy Knight
Tracy Lynge
LTC Detrick Ousby**

**SSG Jorge Ramos
Shatara Riis
Bill Sherod
SGT Noah Sladek
Robert Snell
Joseph Valladares
Johann Wallace
Ramona Williams**