THE PROFESSIONAL BULLETIN OF THE U.S. ARMY CYBER BRANCH

Gray Space

Cyber & Electromagnetic Warfare Journal

Summer 2025

Headquarters, Department of the Army
Approved for public release; distribution is unlimited
PB 2014-25-1

In this Edition

Gray Space

Editor-in-Chief / Harding Fellow:

Capt. Vincent Kirk

The Convergence of Effects: Embracing the New Frontier

Fellow Gray Space Warriors and Defenders of the Nation,

Today marks the inaugural issue of *Gray Space,* a publication dedicated to the evolving landscape of cyberspace operations and electromagnetic warfare. As we stand at this critical inflection point in military history, it is both fitting and necessary that we carve out this intellectual space—a forum where practitioners, theorists, and leaders can collectively forge the doctrine that will shape our future domain and battlespace.

Cyberspace and the electromagnetic spectrum represent not merely new battlefields, but an entirely new paradigm of warfare. The Soldier who once relied on the rifle and bayonet now wields algorithms and waveforms with equal necessity. Our adversaries have recognized this shift; their investments in these capabilities speak volumes about the battlespace of tomorrow. To remain lethal, we cannot cede this territory.

A growing recognition of the transformative power of contact – and the critical role of cyber and electronic warfare within it – is beginning to reshape how Army senior leaders view these capabilities. Yet we find ourselves at a curious juncture. Our military culture, steeped in traditions dating back centuries, sometimes struggles to incorporate these invisible domains with the same reverence afforded to land, sea, and air. How often have we heard cyber and EW capabilities described as “enablers” rather than warfighting functions in their own right? How frequently have we witnessed the most talented digital operators leaving our ranks for civilian opportunities, taking with them irreplaceable institutional knowledge? This shift in understanding is vital, but challenges remain in fully integrating these essential skills and retaining the professionals who possess them.

This publication stands to drive awareness and inspire innovation. To cultivate a culture, both inside and outside of the Cyber Corps, which understands the importance of cyberspace and electromagnetic spectrum maneuver on the battlefield of today, tomorrow and the future. We assert unequivocally that mastery of cyberspace and the electromagnetic spectrum is not peripheral to the profession of arms—it is central to it, which is on display daily in current conflicts. The operators who map network topologies, who craft precise electromagnetic attacks, who defend our critical information infrastructure—these professionals are warfighters in every sense, deserving of the same professional respect and development afforded to every combat arms specialty.

In these pages, you will find not merely technical discourse, though that certainly has its place. You will discover the emerging art of war for the digital age. You will encounter ethical dilemmas unique to operations where effects can be instantaneous yet potentially reversible, widespread yet surgically employed. You will explore how centuries-old principles of warfare manifest in domains measured in milliseconds and megahertz.

We launch this publication with a challenge to every reader: Be stewards of this evolving profession. Contribute your insights, question established assumptions, and mentor the next generation of operators. The doctrine we develop today will determine our readiness tomorrow.

Our adversaries do not distinguish between kinetic and non-kinetic effects—they seek advantage through any available vector. Neither should we create artificial barriers between these domains. The electromagnetic spectrum and cyberspace represent the connective tissue that binds together all warfighting functions. Without dominance there, superiority in any physical domain becomes increasingly tenuous.

The pages that follow represent the collective wisdom of practitioners who have witnessed the evolution of these capabilities from curiosities to critical functions. Their experiences—your experiences—form the foundation upon which we will build a force ready to defend our nation across all domains.

As we move forward together, let us embrace the axiom that has guided military professionals throughout history: we must prepare for the conflicts of tomorrow, not merely perfect our execution of yesterday's wars. In cyberspace and across the electromagnetic spectrum, that future has already arrived.

In service and solidarity,

Col. John J. Hosey
6th Chief of Cyber and U.S. Army Cyber School Commandant

Embracing the Constant: Navigating Transitions as a Soldier

As a Sergeant Major, I frequently interact with Soldiers navigating significant life changes, and one thing remains consistently clear: **transition is the constant in a military career.** From initial entry training to permanent duty stations, deployments, reclassifications, and ultimately, separation – the Army is built on a foundation of adaptation and change. Understanding this, and proactively developing the skills to navigate these transitions, is crucial for both professional success and personal well-being.

As our Army and our Branch continue to implement significant changes within our force and command structures over the coming months and years, it's easy to feel overwhelmed. Uncertainty can breed anxiety. However, recognizing that these shifts are *normal* and *expected* is the first step towards embracing them. The Army intentionally cultivates a dynamic environment – it's designed to forge resilient, adaptable leaders.

Why is flexibility so vital?

- **Operational Effectiveness:** On the battlefield, rigid adherence to plans is a recipe for disaster. Soldiers must be able to think on their feet, adjust to evolving circumstances, and maintain mission focus in the face of the unexpected.
- **Personal Growth:** Stepping outside of your comfort zone, learning new skills, and experiencing different environments foster personal and professional development. Each transition presents an opportunity to expand your skillset and broaden your perspective.
- **Anti-Fragility:** Successfully navigating change builds resilience – the ability to bounce back from adversity. But we can take it further and embrace change as an opportunity for growth. This is arguably the most valuable asset a Soldier can possess, both during and after their service.

How can you prepare?

- **Proactive Planning:** Don't wait for change to happen to you. Actively seek information about upcoming transitions, utilize available resources, and start planning early.
- **Skill Development:** Focus on developing transferable skills – communication, problem-solving, leadership, and critical thinking – that are valuable in any environment.
- **Network Building:** Maintain strong relationships with peers, mentors, and leaders. A strong network provides support, guidance, and potential opportunities during times of transition.

Ultimately, a successful military career isn't about avoiding transitions, it's about *mastering* them. By embracing flexibility, proactively preparing, and cultivating an anti-fragile mindset, you can not only navigate these changes effectively but thrive throughout your service and beyond.

Command Sgt. Maj. Kevin D. Flickinger
6th Regimental Command Sergeant Major
Defend! Attack! Exploit!
Defend! Dominate! Assure!

The Warrant Officer of 2025 and Beyond

When I joined the Army in the late '90s, warrant officers were a different breed. We were the epitome of silent professionals, rarely seen but always present when a technical issue demanded deep expertise. There were no Command Chief Warrant Officers; we didn't sit next to the commander. We were in the trenches, solving problems commanders hadn't yet identified.

Our currency was technical depth.

Today, when I speak to warrant officers, especially those in the Cyber Branch, I emphasize that the Army now requires more from us. Our new currency isn't solely technical prowess, it's influence. While technical expertise remains our foundation, the Army is codifying new titles and responsibilities, such as the Command Chief Warrant Officer, Chief Warrant Officer of the Branch, and Regimental Chief Warrant Officer.

Influence Equation: Self-Awareness / EQ + Trust / Reputation + Performance / Technical Prowess = Ability to Influence

Let's break this down:

- **Self-awareness and Emotional Intelligence (EQ)** are the foundations for understanding how we show up, whether in meetings, on teams, or under pressure. A Cyber Warrant Officer who lacks awareness of their own blind spots, biases, or communication triggers will struggle to lead effectively, especially in complex, matrixed environments where influence is often relational.
- **Trust and Reputation** are the currency others use to decide whether to listen when you speak or follow your lead. You earn both not just through time in grade but through consistency, discretion, and integrity.
- **Performance** keeps you credible. Even if you're technically gifted, your influence erodes if you can't deliver under pressure. Finally, **Technical Prowess,** our traditional strength, remains essential, but it's no longer enough. The Army needs warrant officers who can translate that technical depth into actionable insight for commanders and operational impact for the mission.

When these elements work together, they produce a warrant officer whose voice carries weight, not just because they "know their stuff," but because they've built trust, credibility, and presence to drive outcomes.

Preparing Your Rucksack

The Army prepares warrant officers to be technical experts, fostering depth in specific domains. However, areas like self-awareness and emotional intelligence are still developing within our cohort. As we modernize Professional Military Education (PME), here are three books every warrant officer should add to their rucksack:

- **Atomic Habits by James Clear**:
  Why it matters: We must start with ourselves before advising others. This book offers practical strategies to build good and break bad habits, essential for personal and professional growth.
- **The Color of Emotional Intelligence by Farah Harris**:
  Why it matters: Emotional intelligence is an underrated competency every leader needs. This book explores EQ across diverse populations, mirroring the diversity within our Army.
- **Leadership and Self-Deception by the Arbinger Institute***:*
  Why it matters: As warrant officers, we are advisors and technical leaders. This book delves into self-deception and how it can hinder our leadership effectiveness.

The warrant officer of 2025 and beyond must look beyond purely our technical prowess. By utilizing these resources and focusing on developing our EQ, trustworthiness, reputation, and performance, we can influence and lead effectively in the modern Army.

Defend! Attack! Exploit!

Chief Warrant Officer 5 Brian D. Matthews

Regimental Chief Warrant Officer

Beyond Black & White: *Gray Space* Launches, Pioneering a New Era for Cyber

Capt. Vincent Kirk
Editor, Cyber Center of Excellence

I am honored to serve as the first Harding Fellow for the Cyber Center of Excellence and to lead the development of Gray Space. Transitioning from a Signal background presented challenges, but the journey has been enriching. I am eager to foster thought-provoking discussions and bridge the gap between senior leaders and frontline Soldiers.

The cybersecurity landscape continues to evolve, and today's launch of Gray Space marks a pivotal step forward. This publication is dedicated to exploring modern threat intelligence, proactive defense strategies, lessons learned, and mentorship. Cybersecurity has long been framed as a battle between good and evil, black and white—but the reality is far more complex. The most dangerous threats operate in the "gray space," leveraging legitimate tools, exploiting human vulnerabilities, and blurring the lines between offense and defense. *Gray Space* magazine will illuminate this critical zone, delivering unparalleled analysis, actionable intelligence, and a fresh perspective to stay ahead of emerging threats.

The Harding Fellowship, established in honor of Maj. Gen. Edwin "Forrest" Harding, was created to spark professional discourse and revitalize branch publications during our interwar period. As a major, Harding served as an editor of the *Infantry Journal*, publishing articles that advanced professional infantry tactics and prepared Soldiers for future conflicts. I aim to cultivate that same dynamic within the cyber and electronic warfare communities, building on the legacy Maj. Gen. Harding began.

Once again, the battlefield is shifting as we transition from the Global War on Terrorism to near-peer threats and multi-domain operations. The launch of *Gray Space* signals a bold new direction for cybersecurity journalism—a shift designed to reshape organizations and maintain a strategic edge in the ever-evolving digital battlespace.

Above all, success depends on active engagement from all cyber warriors. Every Soldier in cyber and electronic warfare should seize the opportunity to be heard, share knowledge, and contribute to the force. We look forward to collaborating with each of you to amplify personal experiences, lessons learned, knowledge gaps, and mentorship!

Live Long and Prosper!

Welcome to Gray Space!

Army Cyber Corps - A Prehistory

By Scott Anderson - Cyber Corps Branch Historian

On September 1, 2024, the U.S. Army Cyber Corps turned ten years old. Some may chuckle at the thought of this branch still teetering on the verge of adolescence compared to the more grizzled veteran branches like Infantry, Field Artillery, and Signal just to name a few. However, there is more than meets the eye with cyber, and as I communicate to my students at the U.S. Army Cyber and Electromagnetic Warfare School (which also turned ten) at Fort Eisenhower, GA, the Cyber Corps has accomplished much in its first decade. While still a pre-teen so to speak, the rate of change in this domain has always necessitated that Cyber act mature for its age. What follows is the first part of a planned series chronicling the history of the U.S. Army Cyber Corps and its school. This first essay provides a general synopsis of the emergence of cyber and how it became a key focus for the U.S. military, tracing its early connections to information warfare and operations. It also details the origins of cybersecurity, alongside the creation of Army Cyber Command and West Point's Army Cyber Institute. Finally, a major theme of this essay focuses on the cyberspace areas of concentration developed by the Army Military Intelligence and Signal branches – setting the stage for the eventual adoption of cyber as a standalone career field for Army personnel.

The seeds of this domain germinated in the 1960s as the U.S. military began piecing together computer networks to speed up information sharing and threat detection in the midst of the ever present Soviet nuclear threat.[1] Additionally, throughout the 1960s and 1970s, the NSA had hundreds of "internetted" terminals.[2] It was during this environment of early networking capabilities that the Advanced Research Projects Agency Network (ARPANET) first came online in 1969.[3] By 1976, "Information War" as it pertained to the information flow between weapons systems and the possible digital disruption of Soviet command and control, was viewed as a worthy pursuit.[4] By 1979, NSA leadership recognized that any computer system could be breached by a knowledgeable user, and ideas about "deep penetration" technical capabilities against U.S. adversaries began to take root.[5] By 1986, and possibly earlier, Special Access Programs overseen by the Joint Chiefs and National Security Agency (NSA) began attempting computer network exploitation.[6] As the opportunities for intrusion into adversary networks widened, the U.S. discovered in 1986 that the Soviets were paying hackers to engage in similar tradecraft against U.S. networks.[7]

UCLA DAILY BRUIN

Summer Quarter, No. 9 — UNIVERSITY OF CALIFORNIA, LOS ANGELES — Tuesday, July 15, 1969

Regents set experimental class policy

Guest lecture ruling eased

Country's computers linked here first

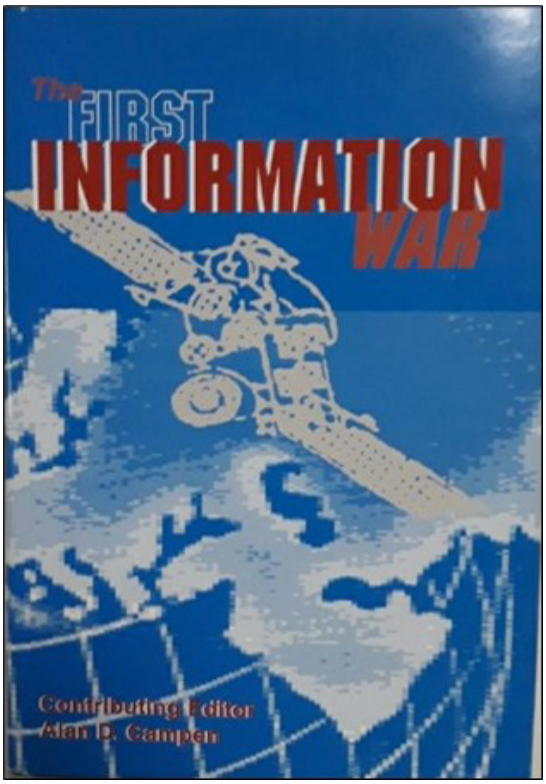
Squeeze on building funds halts campus construction

Open UPC meeting disputes selection of radical members

July 15, 1969: UCLA campus newspaper heralding the first dedicated ARPANET connections between UCLA and Stanford.

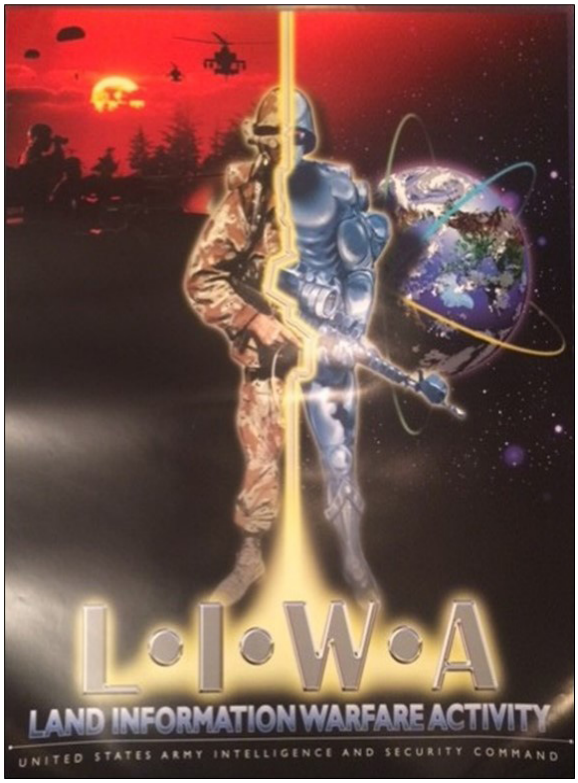
As the proliferation of computer networks spread globally and the ability of these computers to collect, sort, and analyze information at higher speeds, the Department of Defense (DOD) increasingly recognized the high value of information at the strategic and tactical levels of war. During the Gulf War in early 1991 (Operation Desert Storm), information played a crucial role, both in providing Allied forces with enemy intelligence and in disrupting enemy command, control, and communications. Both advantages were greatly increased by technology and computing power, and as one observer declared, "in Desert Storm, knowledge came to rival weapons and tactics in importance…" Unseen, but implicit

in the glowing Desert Storm after action reports, were the information systems – "networks of computers and communications that synchronized the awesome air campaign and that turned dumb bombs into sure-kill weapons."[8] This set the stage for the DOD's focus on the power of information and further exploration on the role computers could play in this sphere.



Alan D. Campen, ed., The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War, 1992.

The growing emphasis on computing power and information as a force multiplier dovetailed with the end of the Cold War and the collapse of the Soviet Union in late 1991. With a reduction in defense spending, the Army capitalized on the idea that information dominance could utilize the latest networks, systems, and sensors to gain information superiority while also economizing force in an era of reduced budgets and manpower. For the next several years, the DOD and Army produced doctrinal concepts ranging from Information Warfare, Command and Control Warfare, and Information Operations (IO). For the Army, this culminated in the activation of Land Information Warfare Activity (LIWA) in 1995 at Fort Belvoir, VA. LIWA had personnel engaging in elements of what we now call Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO). The international peacekeeping operation in Bosnia integrated information operations personnel with maneuver staffs, and the success of these missions demonstrated the importance of IO. In order to maintain the permanence of such skilled IO staff, the Army created the first IO career field with Functional Area (FA) 30 in 1997.[9]

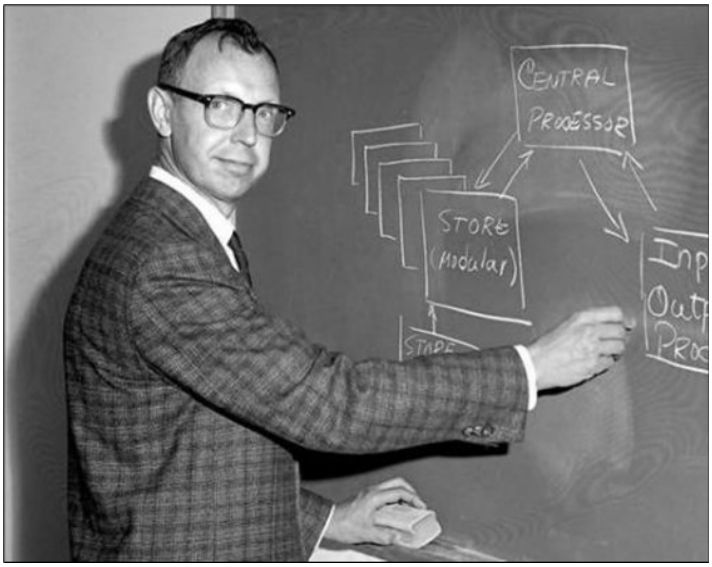


The first LIWA recruitement poster. It was also known as "Cyber Steve" amongst those in the unit.

While LIWA and the IO community played a large role in forming the concepts and framework of cyberspace within the Army, the Military Intelligence (MI) branch was instrumental in developing the actual cyberspace capabilities associated with OCO today. In the 1990s, the intelligence community began correlating computer network operations within foreign computer networks as another form of signal intelligence (SIGINT). With this mindset, the Army's SIGINT brigade (704th MI BDE) created a small unit to focus on cyber warfare in 1995; in 1998, B Co, 742d MI BN was tasked to focus on computer network operations. This begat "Detachment Meade" in 2000 – a unit starting with about three dozen Soldiers. Detachment Meade retained a close relationship with LIWA, which by 2002, had been redesignated as 1st IO Command. Over the next decade, the

Army OCO unit at Fort Meade grew and changed names often. By 2008, the Army Network Warfare Battalion had close to 200 members. It grew into the 744th MI Battalion and finally culminated in today's 780th MI BDE (Cyber) in December 2011.[10]

Underpinning all this cyber activity, was the vital need to maintain the security of U.S. digital property. In 1967, RAND computer scientist, Willis Ware issued a clarion call for the military to beef up security of these new networking capabilities.[11] After becoming the Computer Security Task Force lead, Ware further warned U.S. officials in 1970 that corrupt insiders and spies could actively penetrate government computers and steal or copy classified information.[12] In the days before computer networks were regimented into



Dr. Willis Ware (1920-2013)

the various classifications we are familiar with today, those with prying eyes had easier access to data they had no business reading.

The Signal Corps utilized and maintained computers early on but became increasingly involved as computers became ubiquitous within the Army and essential for communications devices, whether via email or other network-centric methods. Signal's role with network defense was emphasized after the 2002 activation of Network Enterprise Technology Command (NETCOM), where it assumed the role of Army proponent for network defense. However, complexities within the chain of command for cyber defense kept this from being a streamlined process. Army Computer Emergency Response Teams (CERTs) received mission priorities from NETCOM, but 1st IO Command operationally controlled the defenders. Additionally, Signal culture shaped the priorities of those working within cyber defense. Network defense and network maintenance are inherently different. The former identifies and seeks to defeat threat actors while the latter strives for information assurance through securely maintained networks and is less concerned with outside threats. The aforementioned culture of signaleers leans hard toward the goal of properly functioning networks. Network defense might hinder network assurance, and this mentality contributed to keeping the two spheres distinct.[13]

While the Joint Chiefs of Staff labeled cyberspace a "domain" of military operations in the 2004 *National Military Strategy*, the Army continued mapping out its overall cyber strategy. A few years prior to this in 1998, the Army designated Space and Missile Defense Command/ Army Strategic Command (SMDC/ARSTRAT) as the higher headquarters for cyberspace activity. A decade later, in 2008, the Secretary of Defense (SECDEF) directed the different services to establish cyber commands, and the following year, SMDC/ARSTRAT created an interim unit called Army Forces Cyber Command (ARFORCYBER).[14] As the various Army subcommunities already conducting different aspects of the cyber mission (INSCOM, NETCOM, SMDC/ ARSTRAT) jockeyed for lead of this new interim unit, SECDEF Gates announced the creation of U.S. Cyber Command (USCYBERCOM) in June 2009. Per Gates' memo, the service branches needed to establish component commands to support USCYBERCOM by October 2010.[15] Now the Army reoriented its focus on meeting this requirement, which resulted in the activation of Army Cyber Command (ARCYBER) as a new three-star command on October 1, 2010.[16] The first two ARCYBER commanders held combat arms backgrounds, strongly suggesting that the Army sought leaders who could bring fresh perspectives disconnected from the tribal feuding between the intelligence and signal communities.[17]

In the year prior to ARCYBER's activation, the Army Training and Doctrine Command (TRADOC) Commander, Gen. Martin Dempsey, re-

leased a memo in 2009 summarizing a Combined Arms Center (CAC) led working group's findings on how the Army should organize cyber, electronic warfare (EW), and information operations. Based on the group's analysis, Dempsey did not recommend the creation of a new cyberspace career field, opting to retain the status quo of relying on the MI and Signal fields to perform the functions of offensive and defensive cyberspace respectively. Shortly after the activation of ARCYBER and the continued lack of a separate TRADOC governed cyberspace career field, ARCYBER assumed force modernization proponency for cyberspace.[18]

Even after the creation of ARCYBER and its authority over Army cyberspace proponency, leaders continued to favor the model whereby cyber personnel in the Army held certain Additional Skill Identifiers (ASI) that determined their roles within the cyberspace workforce. The Signal Corps and MI communities still desired more stability within this career field and opted to create new military occupational specialties (MOS) to establish more permanency. The Signal Corps looked to their warrant officer cohort to provide the technical expertise necessary to defend the Army's portion of cyberspace. Announced in 2010, the new 255S – Information Protection Technician would perform Information Assurance and Computer Network Defense measures, including protection, detection, and reaction functions to support information superiority.[19] The MI Branch unveiled the enlisted MOS 35Q in the Fall of 2012. Originally called the Cryptologic Network Warfare Specialist, the title later changed to Cryptologic Cyberspace Intelligence Collector. A senior enlisted advisor to the MOS stated: "A 35Q supervises and conducts full-spectrum military cryptologic digital operations to enable actions in all domains, NIPRNet as well as SIPRNet, to ensure friendly freedom of action in cyberspace and deny adversaries the same."[20] The Signal Corps also established an enlisted MOS, 25D – Cyber Network Defender, starting at the rank of E-6, reasoning that "an MOS built on an experienced and seasoned Information Assurance (IA) Noncommissioned Officer workforce, highly trained in Cyber Defense, is the only way to mitigate our vulnerability."[21] The first 25D class graduated from the Signal School in November 2013.[22]

During the first decade of the 21st century, the Electrical Engineering and Computer Science (EECS) Department at West Point advocated for a standalone Army cyber career field. A NSA partnership fueled cooperation and internships between the organizations, and the creation of a cadet cyber security club were just some of the initiatives moving EECS personnel towards advocacy of a new career field. Meanwhile, the EECS program continued training cadets proficient in cyberspace despite not having a branch for them to naturally land.[23] The head of West Point's Cyber Security Research Center, Lieutenant Colonel Gregory Conti, wrote several articles advocating and theorizing about a dedicated cyber work force within the Army. In 2010, Conti and Lt. Col. Jen Easterly contributed a piece on recruiting and retention of cyber warriors within an Army that still did not seem to understand what to do with these specialists.[24] As a testament to the reputation of the EECS department, the Secretary of the Army in 2012 directed the establishment of a U.S. Army Cyber Center at West Point, to "serve as the Army's premier resource for strategic insight, advice, and exceptional subject matter expertise on cyberspace-related issues."[25] This ultimately became the Army Cyber Institute at West Point, which officially opened in October 2014 with Col. Conti at the helm.[26] However, before this occurred, Col. Conti and two EECS instructors, Major Todd Arnold and Major Rob Harrison, wrote a draft theorizing what an Army cyber career path might look like, specifically for officers. While they did not know whether the Army would indeed create a new branch, this detailed study covered multiple courses of action and analyzed the relationships with MI and Signal. The paper even included a proposed cyber branch insignia designed by Arnold and Harrison-with crossed lightning bolts superimposed on a dagger-which ultimately became the basis for the approved insignia.[27]

While the West Point EECS leadership conceptualized the professionalization of a cyber career field, and the MI and Signal branches had created the aforementioned cyber related MOSs, top leadership-including Chief of Staff of the Army (CSA) General Raymond Odierno and General Robert Cone, the Commanding General of Training and Doctrine Command (TRADOC)-was

MAJ Todd Arnold (left) and MAJ Rob Harrison with original Cyber insignia concept sketch at USMA, October 2013.

coming to the conclusion over the course of 2012 and 2013 that the existing split-branch solution was inadequate.[28]

With the approval in late 2012 of the Cyber Mission Force (CMF), it became essential that personnel had the right abilities to go through a very long and exquisite training. Normally, by the time an individual completed this training, they had well over 24 months on station, and as members of the MI or Signal branches, they were often reassigned. Besides the issue of losing skilled personnel due to the normal PCS cycle, Generals Odierno and Cone, as well as many of their subordinates, felt strongly that the cyberspace domain needed to be viewed from a maneuver perspective, which was beyond the MI and Signal Corps' normal mission set.[29] On 20 February 2013, during an Association of the U.S. Army (AUSA) symposium in Ft. Lauderdale, Florida, GEN Cone publicly called for the formal creation of a cyber school and career field. He stated the Army needed to, "start developing career paths for cyber warriors as we move to the future."[30] After GEN Cone's remarks, the wheels were in motion to turn this new school and career field into reality.

Endnotes

1 Called the *Semi-Automatic Ground Environment* or *SAGE*, it consisted of hundreds of radars, 24 direction centers, and 3 combat centers spread throughout North America. For more information, see https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system.

2 Thomas Misa, "Computer Security Discourse at RAND, SDC, and NSA (1958–1970)," *IEEE Annals of the History of Computing* Volume: 38, no.4 (Oct.-Dec. 2016): 17, https://tjmisa.com/papers/2016_Misa_ComputerSecurity.pdf.

3 Researchers at the Advanced Research Projects Agency (now DARPA) created the ARPANET. By 1989, most were calling the network by a more ubiquitous name - "Internet."

4 The Boeing Aerospace Company for the Office of the Secretary of Defense, *Weapon Systems and Information War*, Thomas Rona. (Seattle, WA, 1976).

5 Craig J. Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (PhD diss., George Mason University, Fairfax, VA, 2016), 81; 85.

6 Wiener, "Penetrate, Exploit, Disrupt, Destroy," 93; 98; 352.

7 Clifford Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, (New York: Doubleday, 1989).

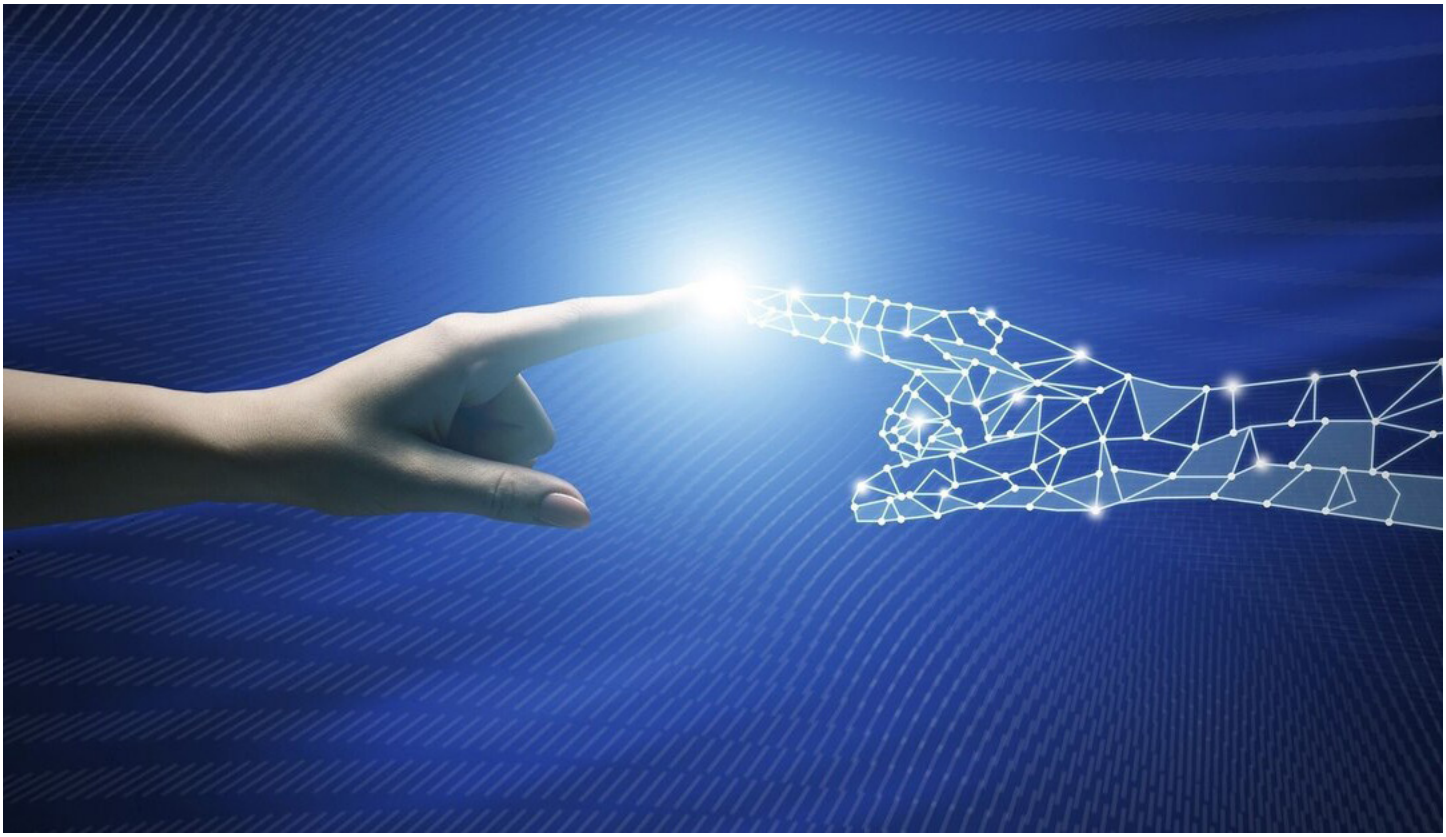
8 Alan D. Campen, ed., The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War (Fairfax, VA: AFCEA International, 1992), x-xi.

9 Maj. Sarah White, "The Origins and History of U.S. Army Information Doctrine," (Thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2022), Chapter 5; Maj. Sarah White, Chapter 3 Edit provided to author from: "Subcultural Influence on Military Innovation: The Development of U.S. Military Cyber Doctrine" (PhD diss., Harvard University, Cambridge, MA, 2019).

10 White, Chapter 3 Edit, 12-16.
11 Willis Ware, “Security and Privacy in Computer Systems” (Paper presentation, Spring Joint Computer Conference, Atlantic City, April 17-19, 1967).
12 The RAND Corporation for the Office of the Director of Defense Research and Engineering, *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security,* Willis Ware. (Washington D.C., 11 February 1970).
13 White, Chapter 3 Edit, 27-29.
14 Ibid., 24-26.
15 Secretary of Defense Robert Gates, Memorandum: “Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations,” 23 June 2009.
16 U.S. Army Cyber Command, “Our History,” https://www.arcyber.army.mil/About/History.
17 White, “Subcultural Influence,” 133.
18 Ibid., 134.
19 Chief Warrant Officer 5 Todd Boudreau, “Repurposing Signal Warrant Officers,” *Army Communicator* 35, no. 1 (Winter 2010): 21.
20 David Vergun, “Army Opens New Intelligence MOS,” *Army.mil*, 30 November 2012, accessed 18 October 2021, https://www.army.mil/article/92099/Army_opens_new_intelligence_MOS.
21 Craig Zimmerman, “SUBJECT: Recommended Change to DA Pam 611-21, Military Occupational Classification and Structure, to Add Military Occupational Specialty (MOS) -- Cyber Network Defender,” (Signal Center of Excellence and Fort Gordon, 30 May 2012).
22 Wilson Rivera, “Cyberspace warriors graduate with Army’s newest military occupational specialty,” *Army.mil*, 13 December 2013. Accessed 20 March 2025, https://www.army.mil/article/116564/Cyberspace_warriors_graduate_with_Army_s_newest_military_occupational_specialty.
23 White, “Subcultural,” 157-160.
24 Lt. Col. Gregory Conti and Lt. Col. Jen Easterly, “Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture.” *Small Wars Journal*, 29 July 2010, https://smallwarsjournal.com/jrnl/art/recruitingdevelopment-and-retention-of-cyber-warriors-despite-an-inhospitable-culture. Jen Easterly went on to become the Director of the Cybersecurity and Infrastructure Security Agency (CISA) from 2021-2025.
25 John M. McHugh, Memorandum, “Establishment of the Army Cyber Center at West Point,” 19 October 2012.
26 Sgt. 1st Class Jeremy Bunkley, “SecArmy officially opens Cyber Institute at West Point, *Army.mil*, 10 October 2014, https://www.army.mil/article/135961/secarmy_officially_opens_cyber_ins.
27 Todd Arnold, Rob Harrison, and Gregory Conti, “Professionalizing the Army’s Cyber Officer Force,” Army
Cyber Center, Vol 1337 No II (23 November 2013); Email between Lt. Col. Todd Arnold and Scott Anderson, 7 November 2018.
28 White, Chapter 3 Edit, 36-37.
29 Mr. Todd Boudreau Oral History Interview with Scott Anderson, 22 February 2021.
30 Unknown Author, “Army leaders see much cyber work to do,” *Taktik(z),* 24 Feb 2013.

Leadership: Artificial Intelligence in Decision-Making

By Lt. Col. Joseph L. Huitt



AI generated illustration

Despite the recent announcement from the Department of Defense (DoD), I posit that Artificial Intelligence (AI) cannot replace the critical *human* factor in leadership decision-making. The Hill recently published an article outlining the formation of a new cell, Artificial Intelligence Rapid Capabilities Cell (AI RCC), whose namesake unsurprisingly gives insight into its purpose.[1] The AI RCC is charged with improving the speed at which the military implements AI technology, focusing on generative AI. What I found alarming was how this new office was going to utilize AI: "command and control, autonomous drones, intelligence, weapons testing, and even for enterprise management like financial systems and human resources."

To frame my argument, it's important to ensure that some terms are defined and put into context. My former boss, Lt. Gen. Stanton, routinely and with much fervor repeated, "you cannot, as a professional in this field (Cyber Corps), use the terms AI or machine learning (ML) without putting them into context." So, what is AI? When thinking of AI, many people conjure up ideas brought to them from the Hollywood big screen, such as robots taking over the world or the AI "Skynet" deciding that humanity is a threat and must be eradicated. However, AI is loosely defined as the ability of machines (computers) to perform tasks that humans do with their brains.[2]

There is also a subset of AI known as Artificial General Intelligence (AGI), which has been slow in development as it seeks to provide machines with comparable human intelligence, able to perform any intellectual task that humans can.[3] Machine learning is a subset of AI and if set up properly, helps make predictions and reduces mistakes that arise from merely guessing.[4] Generative AI is a sub-field of machine learning, capable of developing content such as text, visual depictions, audio, code, and synthetic datasets.[5] Since this is a military-focused article, I would be remiss not to mention *CamoGPT*, which incorporates data from joint and Army doctrine, lessons

learned, best practices [and] Training and Doctrine Command content, among other sources.[6] To understand better, it must be noted that machine learning is made possible by using large language models.

So, what is a large language model (LLM)? LLMs are a category of foundation models trained through data input/output sets using immense amounts of data. This data could have billions of parameters, enabling the LLM to understand and generate content to perform a wide range of tasks. While many are familiar with OpenAI's GPT-3 and 4 LLM, popular LLMs include open models such as Google's LaMDA and PaLM LLM (the basis for Bard), Hugging Face's BLOOM and XLM-RoBERTa, Nvidia's NeMO LLM, XLNet, Co:here, and GLM-130B.

Further scoping my position, this article focuses on two aspects of the AI RCC priorities of implementing AI technology within the Warfighting Functions of Intelligence and Command and Control. Army Doctrine Publication 3-0, Operations, defines a warfighting function as "a group of tasks and systems united by a common purpose that commanders use to accomplish missions and training objectives."[7] Human factors are prevalent in every element of operational planning. From the intelligence officer assessing enemy COAs to the operations officer creating the friendly COAs, and the leader selecting the best course of action, the human element cannot be overlooked.

An example of how the DoD is using AI was an endeavor started in 2017, Project Maven, transitioned to the National Geospatial Intelligence Agency in 2022.[8] Specifically, the project established the "Algorithmic Warfare Cross-Functional Team (AWCFT) to accelerate DoD's integration of [AI]…to turn the enormous volume of data available to DoD into actionable intelligence and insights at speed."[9] This project successfully analyzed massive amounts of data collected from unmanned aerial systems (UAS). The DoD used UAS to capture video feed of the battlefields in Iraq and Syria against the Islamic State; however, it lacked the capacity to process, exploit, and disseminate (PED) the feed in a timely manner, rendering the data useless. The AWCFT created algorithms to review the full motion video (FMV) in near-real time, classifying objects and alerting analysts if there were irregularities.

As a former intelligence officer, the term *intelligence drives operations* (and operations drives intelligence) was repeated often at professional military education and at my assigned units. The Intelligence Warfighting Function is defined in ADP 2-0, Intelligence, as the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment.[10] Intelligence enables *command and control*, facilitates initiative, and allows commanders to develop situational understanding and take decisive action to overcome complex issues that leaders are faced with in today's multidomain battlefield. While intelligence can help lift "the fog of war", what Clausewitz aptly described as unknown factors, it is the leader who is charged with shaping the situation and making decisions to seize the initiative over the adversary.[11]

ADP 3-0 defines the Command-and-Control Warfighting Function as the related tasks and a system that enables commanders to synchronize and converge all elements of combat power. Its main purpose is to assist commanders in integrating the other elements of combat power (leadership, information, movement and maneuver, intelligence, fires, sustainment, and protection) to achieve objectives and accomplish missions.[12] It's easy to grasp why this warfighting function is so critical as it establishes the process to drive operations across all elements of military functions.

If intelligence enables Command and Control, what if the data that drives the intelligence or the data that feeds all warfighting functions becomes corrupted? I agree with Deputy Defense Secretary Hicks that the main reason for integrating AI into military operations is straightforward, it improves decision advantage.[13] However, only one year has passed since the Pentagon unveiled the Data, Analytics and Artificial Intelligence Strategy, and the development of AI in the United States has not advanced to the point where is should transition from improving decision making for military leaders to *allowing* AI technology to *make* decisions—especially in the war fighting func-

tions tasked to the AI RCC charter. In my opinion, these are the most critical among all six warfighting functions, and while technology should be used to assist military commanders, it should not supplant their decision making. There should always be a human-in-the-loop element when it comes to these types of decisions; if not in-the-loop, minimally, humans-on-the-loop should be maintained within the decision-making process where AI is concerned.

The reason that a human must remain in the decision-making cycle is simple: AI can produce false and misleading information and just like any other technology, it can be "hacked." No matter how good the program purportedly is, technology is riddled with security issues—hence the need for routine updates (e.g. patches, protocols, etc.). Recall earlier in the article, LLMs require billions of parameters to be used for the data sets to generate useful information. Not only can these data sets be biased, they can also be unreliable, incomplete, or otherwise undesirable, producing bizarre outputs called hallucinations. Some of these hallucinations can produce false information. Furthermore, humans build the software that drives these AI technologies, and humans are imperfect-they make mistakes. These mistakes create attack surfaces, or opportunities for hackers to take advantage of the mistakes for their benefit.[14]

While there are different motivations that drive hackers, this article will focus on nation states whose cyber operations are ultimately to assist their country in dominating and winning its wars. The adversarial cyber operator could take advantage of the programming mistakes and enable them to purposefully change parameters that the AI technology uses. Recall earlier the great work done by Project Maven: what if an adversary changed the parameters set by the DoD, replacing them with their own? An example could be that the UAS data no longer identifies structures, buildings, personnel, weapons or equipment as intended when using the corrupted AI technology.

Research has already been successful in highlighting ML models are vulnerable to malicious inputs to produce erroneous outputs, which appear unmodified to human observers. Researchers successfully attacked a deep neural network (DNN) hosted by MetaMind and found it misclassified 84.24% of the adversarial examples crafted with its substitute. In their study, the researchers conducted the same attack against models hosted by Amazon and Google, yielding adversarial examples misclassified at rates of 96.19% and 88.94%. Their study also highlighted their approach was capable of evading defense strategies previously found to make adversarial example crafting harder.[15]

Although humans are imperfect beings, the imperfection is why humans remain superior to robots, as they are not constrained by programming and can adapt to unforeseen changes. This is also true for our military, despite being transparent and publishing our tactics, techniques, and procedures (TTPs), our enemies have been baffled when we don't always follow those TTPs on the battlefield. That's because TTPs are merely guidelines, and commanders utilize mission command delegate authority to subordinate leaders, empowering them to accomplish tasks with the given resources and determine the best course of action to meet mission requirements. U.S. history is rich in countless battles where the initiative was seized due to creative leaders at all echelons.

What makes a good leader? Since football terms are often used to understand cyber operations (i.e. offense and defense) the author highlights a quote by the National Football League (NFL) Hall of Fame coach, Vince Lombardi, "Leaders aren't born, they are made and they are made just like anything else, through hard work."[16] Prior to the NFL, Lombardi was an offensive line coach at West Point where he likely learned the foundation of good leadership. ADP 6-22, Army Leadership and the Profession, highlights the characteristics of a good leader. While one can read about leadership, it is through experiences, both successful and failures, that develop leaders, just as Lombardi stated. It takes effort to learn TTPs, conduct battle drills, care for your people, disagree with superiors, and even admit when you're wrong. But these are the qualities that leaders have obtained and sharpened through experiences that enabled them to make decisions.

While AI/ML technologies will certainly continue to ***assist*** our military, there will always be a human factor that cannot be overlooked. Experience, gut feeling, and leadership are all influenced by human factors. Lastly, DoD leaders have routinely stated that the secret to its success, time and time again, boils down to leadership, the ingenuity of our NCO corps, and the ability for leaders at echelon to make decisions.

Even our adversary, Russia, has a U.S. movie based on a true story about a military officer who prevented World War Three during the Cold War; the officer refused to trust their radars that falsely indicated that the U.S. had launched numerous ballistic missiles aimed to destroy them.[17] To continue our military prowess, Artificial Intelligence should never replace the critical *human* element in leadership decision-making. There must always be a human-in-the-loop.

BIO

Lt. Col. Joseph Huitt is a Cyber Warfare Officer, currently serving as Deputy Director, Office Chief of Cyber, U.S. Army Cyber School. He is a graduate of the College of Naval Command and Staff, U.S. Naval War College, and a Distinguished Military Graduate of Augusta University. Lt. Col. Huitt holds master's degrees in Defense and Strategic Studies, and Intelligence Studies. Lt. Col. Huitt has served in leadership positions from the tactical to strategic levels, over his 26-plus years of service. He has gained invaluable experience serving as the Executive Officer to the Cyber Center of Excellence Commanding General; managing Talent at U.S. Army Cyber Command; senior fellow at West Point's Center for Junior Officers; serving as a Team Lead and Battalion Executive Officer within the Cyber Protection Brigade; serving with Special Operations Command in West Africa; serving as Officer-in-Charge within USAFRICOM J2 in England; commanding a Regional Operations Company in the 513th Military Intelligence Brigade; leading first-ever multi-function team in NATO-ISAF in Afghanistan; leading a ground SIGINT platoon in the 66th Military Intelligence Brigade in Germany; deploying in support of USARCENT in Saudi Arabia enabling U.S. invasion into Iraq; serving as a Noncommissioned Officer in Charge at Camp Casey, 2nd Infantry Division in South Korea; and various other stateside units.

References

1. Dress, Brad. "Pentagon Announces New AI Office as It Looks to Deploy Autonomous Weapons." The Hill. December 11, 2024. https://thehill.com/policy/defense/5034805.

2. Potember, Richard. "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD." Federation of American Scientists. January 1, 2017. https://irp.fas.org/agency/dod/jason/ai-dod.pdf.

3. Ibid.

4. IBM Data and AI Team. "AI Vs. Machine Learning Vs. Deep Learning Vs. Neural Networks: What's the Difference?" IBM. July 6, 2023. https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks.

5. "What Is Generative AI?" Innodata. December 14, 2024. https://innodata.com/what-is-generative-ai/.

6. South, Todd. “From CamoGPT to Life Skills, the Army Is Changing How It Trains Troops.” Defense News. October 16, 2024. https://www.defensenews.com/land/2024/10/16/from-camogpt-to-life-skills-the-army-is-changing-how-it-trains-troops/.

7. U.S. Department of Defense. “ADP 3-0 Operations.” Army Publishing Directorate. July 31, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN43323-ADP_3-0-000-WEB-1.pdf.

8. Hitchens, Theresa. “Pentagon’s Flagship AI Effort, Project Maven, Moves to NGA.” Breaking Defense. April 27, 2022. https://breakingdefense.com/2022/04/pentagons-flagship-ai-effort-project-maven-moves-to-nga/.

9. U.S. Department of Defense. “Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven).” National Security Archive. The George Washington University, April 26, 2017. https://nsarchive.gwu.edu/document/18583-national-security-archive-department-defense.

10. U.S. Department of Defense. “ADP 2-0 Intelligence.” Army Publishing Directorate. July 31, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18009-ADP_2-0-000-WEB-2.pdf.

11. Clausewitz, Carl V. 1976. *On War*. Translated by Michael Howard and Peter Paret. Princeton: Princeton Press. https://www.usmcu.edu/Portals/218/EWS%20On%20War%20Reading%20Book%201%20Ch%201%20Ch%202.pdf.

12. U.S. Department of Defense. “ADP 3-0 Operations.” Army Publishing Directorate. July 31, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN43323-ADP_3-0-000-WEB-1.pdf.

13. Clark, Joseph. “DOD Releases AI Adoption Strategy.” Defense. U.S. Department of Defense, November 2, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/.

14. Metz, Cade. “How To Fool AI Into Seeing Something That Isn’t There.” Wired. July 29, 2016. https://www.wired.com/2016/07/fool-ai-seeing-something-isnt/.

15. Papernot, Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami. “Practical Black-Box Attacks against Machine Learning.” Arxiv. March 19, 2017. https://arxiv.org/pdf/1602.02697.

16. “Vince Lombardi.” The Official Website of Vince Lombardi. Accessed December 15, 2024. https://vincelombardi.com/.

17. Harvey, Ian. “The Man Who Saved the World – The Russian Who Avoided WWIII.” War History Online. October 1, 2015. https://www.warhistoryonline.com/featured/real-life-man-saved-world-russian.html.

Artificial Intelligence-Enabled Cyber Education: An Approach to Accelerated Education Development

By Capt. Zachary Szewczyk

I spent almost two years after I left the Cyber Protection Brigade working on training. Not traditional military training like ranges, land navigation, and vehicle maintenance, though, often to my bosses' dismay in the fledgling 3rd Multi-Domain Task Force, but rather cyber training. I wanted to teach my cyber personnel not how to handle a rifle, but rather how to handle big data; not how to read a map, but how to develop a network collection plan; not how to service a vehicle, but rather how to deploy, operate, and maintain a Security Information and Event Management system. The Army has no shortage of M4 experts, yet a worrying shortage of competent network analysts; a plethora of land navigators, yet a troubling dearth of data scientists. Yet little research has tried to answer the question, "How do we build a competent cyber workforce?" We see the consequences of this shortcoming in the news today with frequent discussions of the national cybersecurity skills gap, a problem that affects the military just as much—if not more—than the private sector. Other than vague recommendations to "start with the fundamentals", though, or "buy these seven certifications", little actionable guidance for addressing that gap exists. The fundamentals are certainly important, but what does an aspiring analyst need to learn after they understand networking? Certifications seem to answer that question—just take Network Analyst 2 after Network Analyst 1—but just punt it to someone else—and who is to say they had the right answer, or even a good one?

Analysis of a Defensive Cyber Analyst Education Program

Little research has tried to answer the question, "How do we build a competent cyber workforce?" With few useful leads, I began to research expertise more generally. What is expertise, and how may it be defined? How can a training program facilitate the development of expertise, particularly quickly and at scale? What are the nuances of expertise in the cyber domain?

What started as a few hours of research gradually stretched into days, weeks, and then months. Thousands of pages of reading eventually led to the conclusion that rather than task mastery—the goal of training according to the U.S. Army's Field Manual 7-0: *Training* (2016)—the goal of cyber-specific training ought to be the attainment of expert-level proficiency in domain relevant areas. This is, interestingly, an important distinction that Lt. Gen. John Cushman made back in the 1970s when he advocated for *education* over training, and one with which the first commander of Training and Doctrine Command, Gen. William DePuy, strongly disagreed. (Burke) Task mastery suits static domains with well-defined tasks that are performed under a specific range of conditions and according to fixed standards—but as Cushman correctly predicted about the changing nature of warfare fifty years ago, those strictures have faded such that none of those qualifiers apply to the cyber domain today. The amorphous nature of the cyber domain demands that those operating within it cultivate both routine and adaptive expertise, the abilities to complete well-defined tasks and to solve complex problems in unfamiliar circumstances, respectively. All cyber *education*, then, should seek to develop experts—a specific term for individuals who possess both routine and adaptive expertise and are therefore capable of reliably superior performance in domain-relevant areas as a result. While no single block of instruction will ever accomplish this, all cyber education must share this common goal to make its eventual achievement a reality.

Design of a Defensive Cyber Analyst Education Program

Drawing on operational experience and revised based on extensive research into expertise, I created a defensive cyber analyst education curriculum. This curriculum specifically focuses on developing defensive cyber analysts—a mix of host analysts who specialize in uncovering evidence of malicious activities that occur on endpoints such as user workstations and servers, and network analysts who specialize in uncovering evidence of malicious activity based on

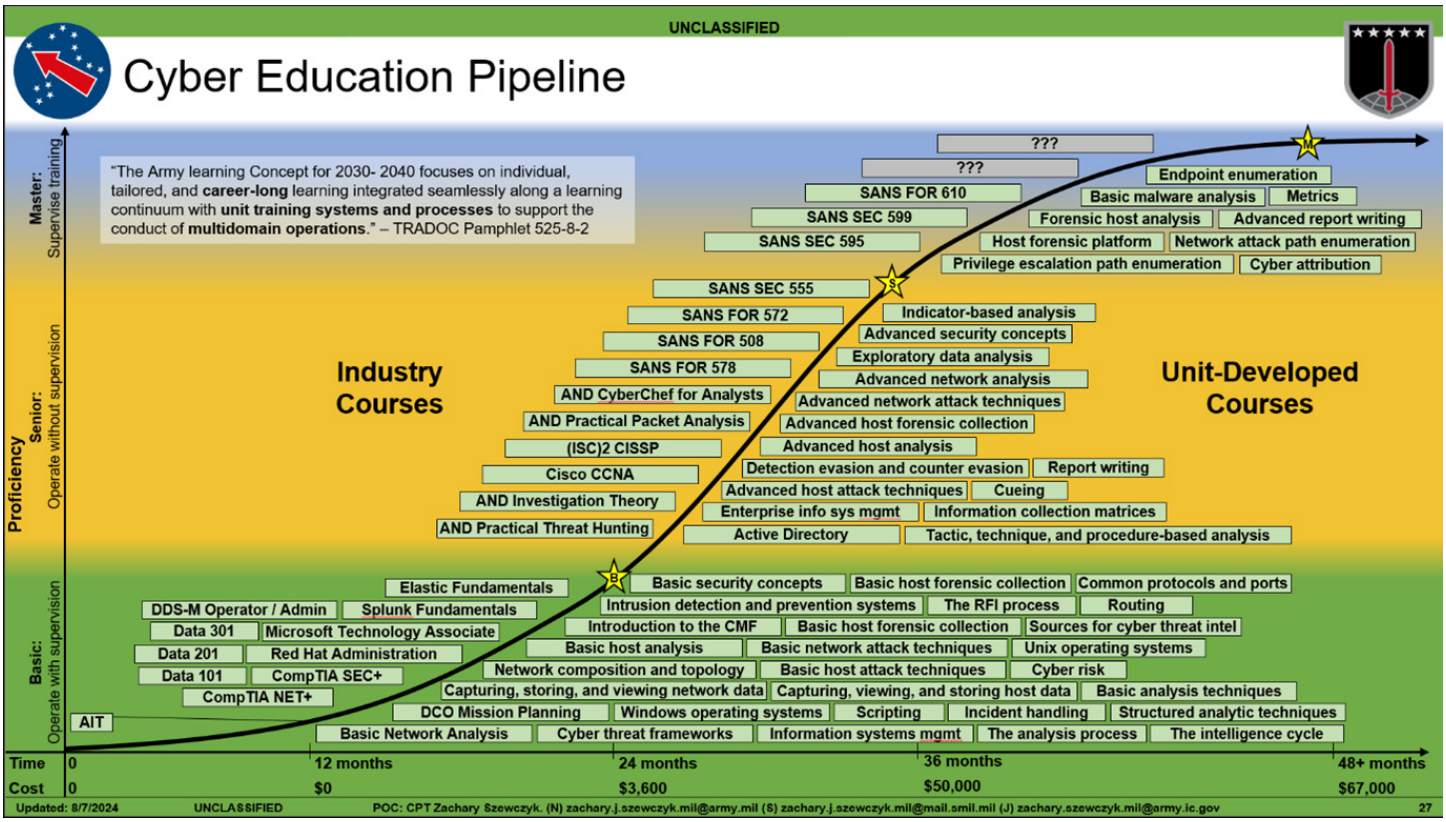


Figure 1: Defensive Cyber Analyst Education Pipeline

communications between those systems over computer networks.

Unit-developed courses, on the right side of the graph, depicts the individual lessons necessary to provide foundational knowledge and skills for defensive cyber analysts to do their jobs. At the basic level of proficiency, in the green band, these focus on developing the analysts' ability to operate under direct supervision. The corresponding industry courses, on the left side of the graph, would support that with foundational cybersecurity knowledge gained through well-known courses and certifications like CompTIA's Security+. While some have, unfortunately, begun to deride introductory-level certifications like Security+ as not worth anyone's time, I still consider these courses and their accompanying certification exams fantastic ways to establish a baseline level of knowledge and prepare individuals for higher level certifications later in their careers.

Senior-level unit-developed courses, in the yellow band, would then develop the analysts' ability to operate unsupervised and provide supervision to other, more junior analysts. The industry courses at this level would focus on work role-specific knowledge and skills through more targeted courses like Applied Network Defense's Investigation Theory and SANS 578: *Cyber Threat Intelligence*. An emphasis on SANS's exquisite offerings will surprise no one in the cybersecurity field, but I also made it a point to consider other, less well-known but similarly high-quality courses from organizations like Applied Network Defense.

Finally, master-level unit-developed courses, in the blue band, would focus on developing the force, while the corresponding industry courses would give the analysts the deep technical knowledge to do so effectively. Many of these courses will come from SANS, at least initially, because it is rightfully considered the gold standard in cybersecurity education for a good reason. Future versions of this pipeline may feature other organizations' courses as well, such as the Naval Postgraduate School's *Data Science Certificate*.

While many other approaches to cyber education exist, mine acknowledges the critical role of internally developed courses when building a competent cyber workforce. Externally developed and hosted courses can be used to complement my curriculum, but they cannot replace it. This approach capitalizes on the Army's long-standing tradition of Soldiers training

Soldiers and avoids the pitfalls of entirely civilian-led education. While a heavy reliance on the private sector does have its merits, it is the wrong decision for the long-term health of the military's cyber forces. Operational insights are almost never available to the public, for one, and the ways, means, and ends of cybersecurity in the military—although similar to the private sector—are not the same.

Manual Development of a Defensive Cyber Analyst Education Program

Unfortunately, a curriculum alone does not make an education program. With a plan in place, though, my small team began developing this material manually. Figure 2, below, depicts the 5-step manual instruction material development model, a product of my own design. Unlike the Army's 8-step training model, which focuses on the execution of training, my model provides guidance for creating the actual instruction material. It starts with conceptualization, then outlining, followed by shell creation, the delivery of an 80% solution, and finally the finished product at step five.

For each of the fifty-four modules on the right side of the defensive cyber analyst education pipeline, figure 1, we wrote a brief module description that consisted of a one-sentence title and a short paragraph describing the module's purpose, key topics, and a desired end state in step one. In step two, we created outlines that logically sequenced each module's topics and included a list of key points within each section. In addition to organizing the module, these outlines would also help instructors stay on track and ensure they covered key points as they taught each block of instruction. From there, we would turn that outline into actual instruction material—often a series of slides interspersed with practical exercises—that culminated in some sort of "check on learning," such as a quiz, in steps three and four. Each module would also feature a handout with leading questions designed to enhance student engagement and facilitate guided note taking.

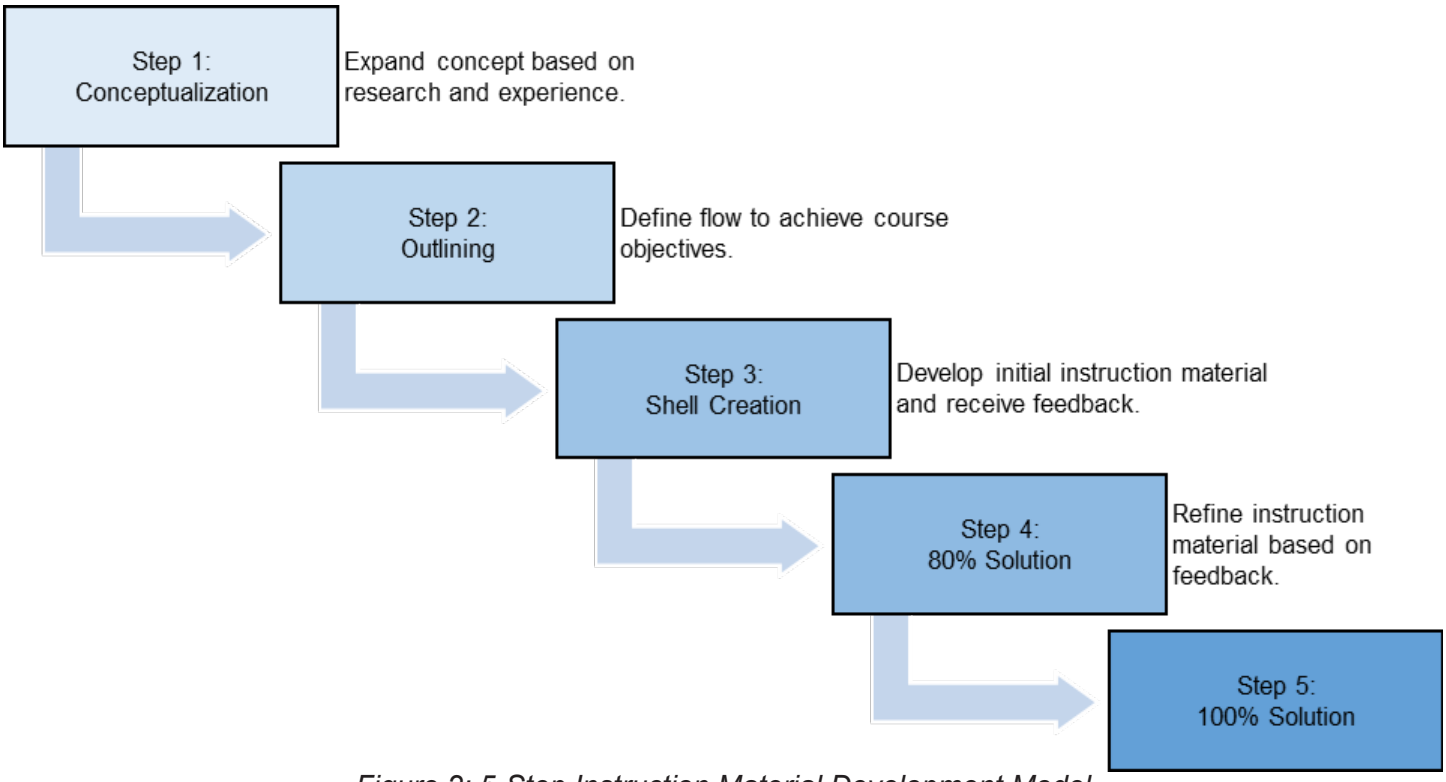


Figure 2: 5-Step Instruction Material Development Model

After an initial attempt to build all the instruction material for the entire defensive cyber analyst curriculum manually, my team estimated almost a year's worth of work to finish creating all fifty-four modules' worth of material. OpenAI's ChatGPT had grown astonishingly capable by this point, and we began exploring ways to accelerate that time-consuming development process with artificial intelligence.

Artificial Intelligence-Enabled Development of a Defensive Cyber Analyst Education Program

Our first foray into integrating artificial intelligence into the instruction material development process had it absorb steps one, two, and three of my 5-step process: conceptualization, outlining, and shell creation. Given a module description, a large language model like OpenAI's Generative Pre-trained Transformers (GPT), via the ChatGPT web interface, would expand that description into an outline. This allowed an artificial intelligence agent to complete the initial, cursory research that fed into outlines, and attempt to logically sequence them in a coherent manner. While this seldom produced a perfect outline, it often resulted in a partial solution that one of my "course designers" could finish in short order.

Initially, this approach seemed extremely promising: in just two weeks, we used a mix of ChatGPT and Bard, a competitor to OpenAI's GPT models from Google, to create outlines for all fifty-four courses. While at first this approach seemed promising, it did not address the true limiting constraint of this process.

$$P = \frac{0.15 \times \text{Outlines} + 0.75 \times \text{Slides} + 0.10 \times \text{Handouts}}{\text{Number of Soldiers} \times \text{Number of Hours}}$$

Figure 3: Productivity Equation

Figure 3, depicts an equation I developed to measure productivity. It weighs products by the approximate amount of effort required to produce them and then calculates a rough measure of productivity as a function of products generated divided by person-hours invested to create them. When I plugged in the numbers from our first and second iterations of instruction material development, the results confirmed my suspicions: limited artificial intelligence integration had improved our productivity over the strictly manual process, but not enough to make a significant difference.

In his 1984 book, *The Goal*, Eliyahu Goldratt introduced the theory of constraints. This theory holds that a small number of constraints—or "bottlenecks"—will limit the overall productivity of a system. In one of my favorite books, *The Phoenix Project*, Gene Kim explained this theory's applicability to business processes: "Any improvements made anywhere besides the bottleneck are an illusion. Any improvement made after the bottleneck is useless, because it will always remain starved, waiting for work from the bottleneck. And any improvements made before the bottleneck merely results in more inventory pilling up at the bottleneck." In our first foray into artificial intelligence-enabled instruction material development, we had optimized for the wrong constraint!

Artificial Intelligence-Driven Development of a Defensive Cyber Analyst Education Program

Fortunately, by then I had begun a skunkworks project to tackle the true limiting constraint: the slides. Donald Knuth's TeX typesetting language, which I used to write a guide for cyber operations called *The Handbook for Defensive Cyberspace Operations*, could also generate slides thanks to the immensely powerful Beamer package. After some tepid experimentation, I decided to dive in.

Over the course of a few hours, I developed a professional slide template in LaTeX, an extension of Knuth's typesetting language. Based on that template, a few lines of text such as those in figure 4, would now generate a PowerPoint style slide with a header, footer, unit logos, classification banner, classification markings, a title, and a bulleted list in the body.

```
\section{Title \& Content TOC Title}
\begin{frame}{Title \& Content Slide Title}
  Basic title and large, main body content
slide.
  \begin{enumerate}
      \item Item number one.
      \item Item number two.
  \end{enumerate}
  And so on.
\end{frame}
```

Figure 4: Example LaTeX Slide Source

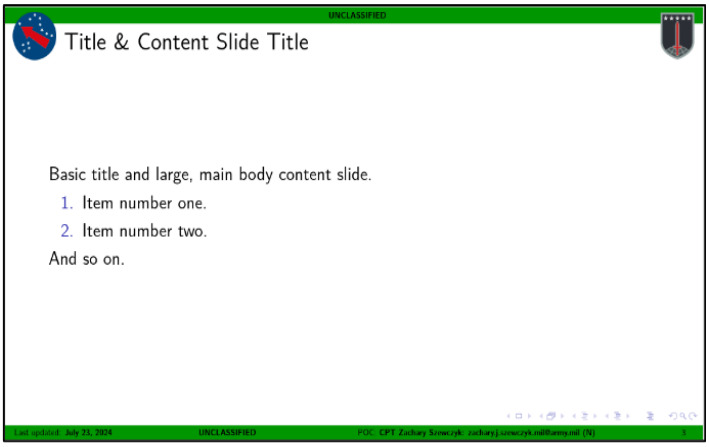


Figure 5: Example LaTeX Slide Output

Figure 5, depicts the output of figure 4's source code. By replacing everything between "\begin{-frame}" and "\end{frame}" I could instead feature pictures, diagrams, flowcharts, tables—anything PowerPoint could do, I could now do with a bit of text. To call this a watershed moment in this project's development would be an understatement. Where we had once painstakingly created diagrams and tables by hand, we could now take advantage of scripting and, critically, large language models like OpenAI's GPT4 to tackle the last true bottleneck constraining this initiative.

After a few weeks of learning to interact with OpenAI's application programming interface, or API, and developing the Python glue that would bind the entire project together, I had a working product. A series of Python scripts could now parse *The Field Guide to Defensive Cyber Analyst Education,* a short manual I wrote that explains the defensive cyber analyst education program I developed in detail, to identify all fifty-four unit-developed courses and their descriptions. The script would then feed those descriptions to OpenAI's GPT 3.5 model to generate an outline. With an outline and a series of related course objectives, the more capable GPT4 model would revise the outline into a more detailed, finished product. GPT4 would also create the handout to accompany the course material. These steps alone underscore the immense power of *generative* pre-trained models, which accepted just under 5,000 words as input and output over 60,000 words in outlines and handouts.

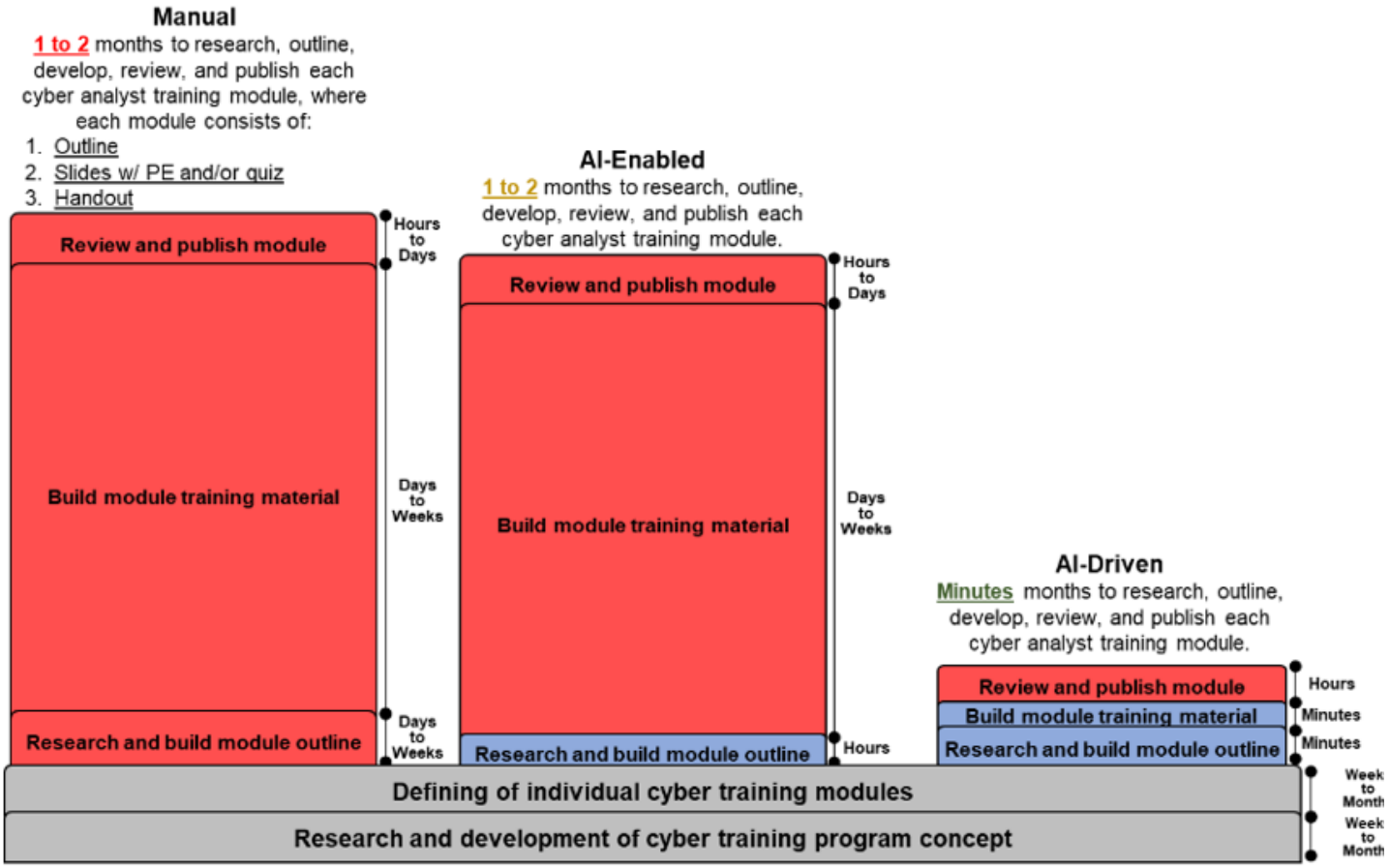


Figure 6: Maunal vs. AI-Enabled vs. AI-Driven Instruction Material Development Process

Finally, the script would read these outlines and iteratively prompt GPT3.5 and GPT4 to generate individual slides. These slides would then be stitched together into a complete presentation using another extension of Knuth's TeX, called XeLaTeX, via the XeTeX engine. Here, the original 5,000 words of module descriptions became 60,000 words in outlines and handouts, which expanded into a staggering 284,000 words on 1,600 slides across 54 presentations in class material. Through scripting and the help of artificial intelligence, we had successfully automated the entire 5-step instruction material development model. Figure 7, compares the three incarnations of the instruction material development process by the approximate amount of time necessary to complete each step: manual, AI-enabled, and AI-driven. What would have taken months under the best of circumstances if done the old, manual way took mere seconds and cost me just $34.68.

Aside from speed, this programmatic, AI-driven approach to content generation also had another benefit: machine-readable data structures and interfaces made transforming content a few minutes' work with a Python script. In addition to generating 54 individual slide decks, this pipeline also generated an accompanying book for each module. Each book contained the same material as the original course content, for those more inclined to learn through reading than by listening to a lecture.

This approach also had other benefits from an administrative perspective, too. For example, compiling all the slides and books into a single document for review by a foreign disclosure officer took a few seconds rather than hours of copying-and-pasting hundreds of slides into "Master PowerPoint v7.ppt". Condensing the outlines into a nice catalog for dissemination to other organizations required a few lines of Python, not hours wrestling with Microsoft Word.

By focusing on and optimizing the correct constraint, I created a process that took months of work and reduced it to just a matter of hours. Figure 8, compares the productivity measures for the three approaches.

$$P_{\text{manual}} = \frac{0.15(15) + 0.75(15) + 0.10(2)}{10 \times 480}$$
$$P_{\text{manual}} = \frac{2.25 + 11.25 + 0.20}{4800}$$
$$P_{\text{manual}} = \frac{13.7}{4800}$$
$$P_{\text{manual}} = 0.002854$$

$$P_{\text{AI-enabled}} = \frac{0.15(54) + 0.75(1) + 0.10(54)}{2 \times 120}$$
$$P_{\text{AI-enabled}} = \frac{8.1 + 0.75 + 5.4}{240}$$
$$P_{\text{AI-enabled}} = \frac{14.25}{240}$$
$$P_{\text{AI-enabled}} = 0.059375$$

$$P_{\text{AI-driven}} = \frac{0.15(54) + 0.75(54) + 0.10(54)}{1 \times 24}$$
$$P_{\text{AI-driven}} = \frac{8.1 + 40.5 + 5.4}{24}$$
$$P_{\text{AI-driven}} = \frac{54}{24}$$
$$P_{\text{AI-driven}} = 2.25$$

Figure 7: Manual vs AI-Enabled vs AI-Driven Instruction Material Development Process Productivity

Artificial intelligence tools like OpenAI's ChatGPT have taken the world by storm. Their sudden popularity, and the accompanying "AI-ification of everything", makes it easy to forget that this technology is still in its infancy. Many organizations, including the Department of Defense, are still exploring appropriate roles for it, and trying to understand its impact. As I look back on the first phase of this project, I have answers to both of those questions, and the results to back them up. Instruction material generation is a fantastic role for AI, particularly when paired with domain experts and used in an iterative manner. I know, because it ultimately led to an 788x increase in our productivity.

Way Forward

As I look back on this project, and the months of research that enabled that execution to succeed, I am immensely proud of how far this initiative has come. I am also excited for the future as I consider all the opportunities to improve and expand this cyber education program.

The current incarnation of this program focuses on U.S. Cyber Command's Host Analyst and Network Analyst work roles. Given the continued difficulty of effective intelligence support to cyber operations, I look forward to expanding its scope to include a cyber threat intelligence analyst capacity as a small step toward remediating that. In a similar vein, I also look forward to exploring what it means to train officers and NCOs in the now-defunct Cyber Network Defense (CND) Manager work role, which the Army unfortunately nixed several years ago. Planning, overseeing, and executing defensive cyber operations has become a responsibility shared by the Cyber Planner and Analytic Support Officer work roles, but I have and will continue to advocate for an important third leg to this stool, the CND Manager, who handles the day-to-day execution of cyber operations, leads analysis, and coordinates incident responses. Fortunately, integrating courses to build cyber threat intelligence analyst and cyber network defense manager capacities will result in a logarithmic increase, not a linear one, thanks to the integrated nature of this program. By designing this program around knowledge domains rather than work roles, adding sufficient materials will require minor course adjustments instead of drastic changes in direction.

I believe this approach has the potential to apply elsewhere as well. Applying a similar artificial intelligence pipeline to areas sorely in need of formal curriculum, such as the electronic warfare specialty, could help grow this nascent field.

Unfortunately, generalizing this pipeline to other work roles—and even other fields—is not without risk. Accelerating the instruction material development process risks flooding the space with low-quality products. Appropriate direction, important now to economize resources, will become critical in a future free of such constraints. Outcome-based learning is the right approach, particularly for cyber where Soldiers must be educated not trained, but the outcomes achieved must become job qualification. Knowledge for knowledge's sake is the purview of academia, not the military.

General-purpose models like GPTs 3.5 and 4, although effective for developing defensive cyber analyst training given the field's significant overlap with cybersecurity in the private sector, are also unlikely to perform well in narrow specialties throughout the military. Fortunately, phenomenal initiatives like CamoGPT will soon provide Soldiers with access to large language models trained on domain-specific information and backed by military doctrine. CamoGPT must, however, be appropriately resourced to support state of the art, frontier models. Many "large" language models, with just a few billion parameters, hardly deserve the name compared to those with trillions of parameters available today. Emergent properties, especially important in ill-structured tasks like training development, do not appear in small models, and only begin to appear in some of the largest models available today. CamoGPT must have the resources to handle these gargantuan models lest it become little more than a toy.

Conclusion

This article's approach represents one of the few attempts to codify and disseminate a formal approach to cyber analyst education, particularly one that views internally developed courses as central to its execution rather than an afterthought. I hope to see other units in the cyber mission force seize this opportunity to collaborate and build upon this program. The Army has no shortage of M4 experts, yet a worrying shortage of competent analysts, and while this program may not be *the* answer, it is certainly a great start.

About the Author

Captain Zachary Szewczyk commissioned into the Cyber Corps in 2018 after graduating from Youngstown State University with an undergraduate degree in computer science and information systems. He has supported or led defensive cyberspace operations from the tactical to the strategic level, including several high-level incident responses. He has served in the Cyber Protection Brigade and the 3rd Multi-Domain Task Force.

Reference

Burke, E. M. (n.d.). Ignoring Failure: General DePuy and the Dangers of Interwar Escapism. *Military Review*, 42–58.

Cyber Center of Excellence and Army Transformation

By Retired Command Sgt. Maj. Michael K. Starrett

Guided by foundational doctrine, such as FM 3-0, the Army is investing in transforming its force structure, equipment, and training to achieve success in multi-domain operations (MDO).

The United States Army is often hailed as the premier fighting force in the world. This distinction is due to a combination of exceptional training and professionalism, advanced technology and equipment, and a global presence. However, maintaining this status requires constant evolution to address emerging threats and operational requirements. As the Army pivots from two decades of counterinsurgency (COIN) operations to prepare for large-scale combat operations (LSCO) against peer adversaries, modernization efforts are taking center stage.

The Shift to Multi-Domain Operations

FM 3-0, Operations, outlines the Army's approach to MDO, emphasizing operations across five domains: land, air, maritime, space, and cyberspace. These operations also span three dimensions—physical, informational, and human—to create a synchronized and comprehensive approach to warfare. LSCO amplifies this complexity, demanding the ability to integrate capabilities across domains to achieve strategic objectives. To meet these challenges, the Army launched a modernization campaign known as "Transformation in Contact" (TiC), intended to enhance its readiness and adaptability while maintaining global mission requirements.

The Cyber Center of Excellence (CCoE) at Fort Eisenhower, Georgia, is fully engaged in this modernization effort. The CCoE is preparing Soldiers to operate effectively in the high-stakes environment of LSCO by addressing force structure adjustments and advancing training initiatives.

Force Structure Modernization

MOS Convergence in the Signal Branch

One CCoE modernization effort involves Military Occupational Specialty (MOS) convergence within the Signal branch. This initiative consolidated 13 MOSs into seven, creating a more versatile and adaptable force. For example, the 25H, Network Communications Systems Specialist, merged four previous specialties: 25N (Nodal Network Systems Operator), 25Q (Multichannel Transmission System Operator), 25L (Cable Systems Operator/Maintainer), and 25W (Telecommunications Operations Chief). By formalizing cross-training practices that units have informally used for years, MOS convergence enhances the Army's flexibility and operational efficiency.

This restructuring streamlines the Signal Corps and provides Soldiers with a broader skill set. For instance, during a 2005-2006 deployment to Afghanistan, Soldiers from the 7th Signal Brigade cross-trained 25L Wire Systems Installer/Maintainers and 92G Culinary Specialists to operate Satellite Transportable Terminals (STT). Such adaptability, through informal cross-training, ensured that network capabilities were maintained in austere environments. Today's MOS convergence institutionalizes this approach, equipping the Army to meet the demands of the modern battlefield.

Growth of the Cyber Branch

Simultaneously, the Army is expanding the Cyber branch to address the growing importance of cyberspace and the electromagnetic spectrum in LSCO. Established in 2014, the Cyber branch (CMF-17) has grown rapidly, increasing authorizations by over 1,800 positions between 2016 to 2024, with plans to add another 500 by 2030. Much of this growth is concentrated in the 17E MOS, Electronic Warfare Specialist, reflecting the branch's focus on offensive and defensive cyber capabilities.

The Cyber branch mission includes enabling commanders to monitor friendly forces' electronic signatures for force protection and leveraging cyberspace to locate and neutralize adversaries. By integrating cyber and electromagnetic capabilities into operations, the Army can achieve superiority in these domains and gain a decisive advantage over peer threats.

Training Modernization

As the Army's force structure evolves, so too must its training programs. Preparing Soldiers and leaders for LSCO requires a paradigm shift in how the Army delivers education and technical skills development. Recognizing the rapid pace of technological advancement, the Army introduced the Mobile Advanced Readiness Training (MART) concept, which aims to bridge the gap between rapidly emerging technologies and operational readiness. The Army emphasizes leader development as a critical component to mission readiness and essential to fostering a resilient and adaptable force.

Mobile Advanced Readiness Training (MART)

Unveiled by Col. Michael Wacker at the 2024 AFCEA TechNet Augusta, MART represents a flexible and adaptive training model designed to address rapidly changing technology. MART offers 13 lessons across four categories—foundational signal training, collective training, data training, and signal leader training. This structured approach focuses on delivering tailored instruction to meet the needs of operational units across all Army career management fields. The MART training approach ensures Soldiers are equipped to operate the latest systems and technologies, even as those technologies outpace traditional institutional training timelines.

The MART concept embodies the Army's commitment to adaptability. By integrating best practices and lessons learned from the field, MART ensures that training remains relevant and effective. This initiative reflects the Army's broader philosophy of preparing Soldiers to adapt and thrive in unpredictable environments.

Leadership Development

FM 6-22, Developing Leaders, underscores the importance of leadership in the Army's success. As the operational environment becomes increasingly complex, leaders must possess not only technical expertise but also critical thinking and decision-making skills. Modernization efforts in training also extend to leader development, ensuring that commanders at all levels can integrate capabilities across domains and dimensions. Leader development training emphasizing mission command, problem-solving, and ethical decision-making are central to this effort. An example of recently developed leader training is the Signal School's "Data for Leaders Course", emphasizing data analysis and interpretation, data driven decision making, and advanced data strategies.

The Role of Technology in Modernization

The Army's technological edge has long been a cornerstone of its effectiveness. Modernization efforts are focused on enhancing this advantage by developing cutting-edge weapons, vehicles, and communication systems. From hypersonic weapons to resilient communication networks and electromagnetic warfare capabilities, the Army's investment in technology is designed to provide superiority against any adversary.

Cyber and Electromagnetic Capabilities

FM 3-12, Cyberspace and Electromagnetic Warfare, highlights the critical role of these capabilities in LSCO. Army cyber modernization efforts, such as cyber ranges and the Integrated Tactical Network (ITN), aim to deliver both offensive and defensive effects and enable units to shape the battlefield through information dominance. By integrating cyber capabilities into joint and combined operations, the Army can disrupt adversary networks, protect its own systems, and enhance situational awareness.

Artificial Intelligence and Autonomous Systems

Emerging technologies such as artificial intelligence (AI) and autonomous systems are also transforming how the Army conducts operations and trains the force. AI-powered analytics provide commanders with actionable insights, while autonomous systems enhance reconnaissance, logistics, and combat capabilities. In November 2024, the Cyber Center of Excellence launched CamoGPT-CCoE, an AI tool designed to assist CCoE workforce with daily tasks such as developing Programs of Instruction (POI), creating lesson plans, checks-on-learning, and course exams. These advancements in AI increase institutional and operational tempo and reduce risks to Soldiers by delegating dangerous tasks to machines.

Continuous Transformation for Future Success

The U.S. Army's commitment to "continuous transformation" ensures that it remains prepared for future conflicts. This transformation encompasses force structure, training, and a cultural shift toward embracing innovation and adaptability. By fostering a culture of learning and agility, the Army can anticipate and quickly respond to the challenges of an ever-changing operational environment. The CCoE exemplifies commitment to transformation and remains at the forefront of preparing the ARMY for LSCO through MOS convergence, growing the Cyber branch, and developing the MART concept. By integrating lessons learned from past experiences with emerging technologies and best practices, the CCoE ensures that Soldiers are trained and equipped to fight and win in multi-domain environments

Sgt. 1st Class Salvador Pinto teams up with Industry partners to learn the capabilities of new equipment during Cyber Quest 24. (Photo by Lesli Ellis-Wouters, Cyber Center of Excellence)

Strategic Partnerships

Modernization efforts also benefit from collaboration and relationships with industry, academia, and allied forces. Collaboration with industry enables the Army to leverage cutting-edge innovations. A great example of collaborating with industry is the annual AFCEA TechNet Augusta Conference and Expo, where military and industry leaders come together to discuss defense modernization efforts and how industry can contribute. Joint training exercises with allies enhance interoperability and strengthen relationships. These relationships are critical to ensuring the Army remains at the leading edge of military innovation.

Conclusion

The U.S. Army's modernization efforts are a testament to its dedication to maintaining superiority in an increasingly complex and contested world. By transforming force structure, enhancing training, and leveraging technology, the Army is preparing for the challenges of LSCO and MDO. Guided by foundational doctrine and driven by a commitment to adaptability, the Army ensures that it remains ready to deter aggression, defend the Nation, and secure victory in any domain.

As the United States Army celebrates 250 years of service to the Nation, its legacy of excellence continues to inspire confidence in its ability to meet the demands of future conflicts for decades to come.

Forge and Project Power!

Integrating Cyber Protection Teams into Training Exercises

By Col. Jon Erickson

Col. Jon Erickson, 335th Signal Command Cyber Director

The 86th Training Division plans, delivers, and enables realistic and relevant training in complex and austere training environments to prepare commanders, Soldiers, and units for multi-domain large scale combat operations (LSCO). This type of training is only available to most Army Reserve units at the Combat Support Training Exercise (CSTX) in Fort McCoy. In recent years, CSTX has been the center of innovation, where over 7,000 Soldiers have been exposed to new capabilities and delivered feedback to the capability providers. New to the CSTX, was the participation of the Army Reserve Cyber Protection Brigade (ARCPB).

Incorporating a CPT into a Training Exercise:

As part of the exercise scenario, the CSTX division commander's G6 submitted a request for forces (RFF) for a Cyber Protection Team (CPT) to mitigate a cyber-attack that the division was experiencing. The ARCPB assigned CPT 183 to serve under the operational control of the CSTX division commander. CPT 183 received an order from the G6 to determine what vulnerabilities were exploited and recommend how the G6 can prevent future attacks from succeeding. CPT 183 employed their virtual Deployable Defensive Cyberspace-Modular kits in the Persistent Cyber Training Environment (PCTE) cyber range to conduct initial network reconnaissance, identify cyber key terrain, uncover what vulnerabilities were exploited, and determine the enemy's most likely and most dangerous courses of action. Their final task was to brief the Division G6 on best practices and the actions required to prevent future cyber intrusions.

CPT 183 is assigned to the Southwest Cyber Protection Center (SWCPC) at Fort Gillem, GA and participated in CSTX during their Battle Assembly training from Aug. 3-4. The 86th Training Division's Cyber Observer, Coach/Trainer (OC/T) team initiated the cyber exercise and managed the event through PCTE. As CPT 183 accomplished specific cyber tasks in PCTE, these activities were captured and simulated in the Cyber Battlefield Operating System Simulation (CyberBOSS) platform. This training exercise demonstrated three concepts that should be value added for the Army moving forward. The first concept was demonstrating that cyber training events can be executed remotely and linked to Army Reserve Collective Training Exercises. The second concept proved that OC/Ts are capable of remotely observing and evaluating a CPT's performance during their missions. The third and final concept was demonstrating how CPTs across the force can receive technical training value when partnering with other units during training events.

Due to CPT 183's participation, the 86th conducted a first-of-its-kind proof of concept that overcame several technical hurdles and captured

live cyber activities on a cyber simulation platform. Maj. Eric Fong, the 86th's cybersecurity engineer, partnered with Program Executive Office – Simulation, Training, and Instrumentation (PEO-STRI) and U.S. Army Combat Capabilities Development Command (DEVCOM) to receive activities from PCTE and accurately capture and replicate CPT activities in near real-time in CyberBOSS. The main goal of inserting a CPT into a CSTX was to demonstrate that a blended cyber-kinetic training exercise more realistically depicts the modern warfare scenario. Current practice for training exercises will simulate defensive cyber actions by creating an inject in the Master Scenario Event List (MSEL) and handing it to the training audience as a "white card". The "white card" simply states what the cyber-attack is conducting on the network without any effects. Participating CPTs can conduct near real-time defensive operations which will impact the training audience and drive what MSEL injects to execute.

According to the SWCPC commander, Lt. Col. Eric Booker, "Cyber Protection Team 183's participation in the exercise allowed me as a commander to observe the team operate on collective tasks. Moreover, I was able to watch junior officers and NCOs lead in a small group setting. The back brief session alone was invaluable training for the Soldiers as it gave them practice in briefing the network owners on mission findings. Great training conducted by Soldiers from their home station!" CPT 183's participation allowed developers for PEO-STRI and DEVCOM to observe how a CPT operated on a mission, receive feedback on how the exercise went, and determine the direction for future enhancements.

Way Ahead:

Building upon the success of this proof of concept, the next step is for the Cyber OC/T team to collaborate with G6 and DEVCOM to create scenarios within CyberBOSS that can directly affect the exercise network. Adding this capability to the current proof of concept would create a fully integrated, end-to-end Live, Virtual and Constructing (LVC) system into the exercise. CyberBOSS would function as the conduit linking the virtual effects in PCTE to the live effects on the exercise network. Where a certain cyber effect may create too much risk to either the network or to training units, CyberBOSS can be used to execute the effect in its sandbox environment to create constructive effects that drive what MSEL injects to implement.

One final initiative for creating a fully integrated LVC system is to allow other training exercises and training divisions to receive the benefit of a CPT's participation. As the Division G6 is tasking the CPT to conduct various missions in PCTE, CyberBOSS would capture all CPT activities and emulate those activities in the cyber simulation platform. In future training exercises where a CPT may not be available, the training division could employ a virtual CPT that is emulated by CyberBOSS. This type of capability would allow any training exercise the benefit of incorporating a constructive CPT into its scenario and to choose what CPT missions to execute in the exercise.

Bio

Col. Jon Erickson, is a Cyber and Signal officer and a Functional Area 26B (Information Systems Engineer) in the U.S. Army Reserves serving as the Cyber Director for the 335th Signal Command (Theater). He is a graduate of the Army War College. His previous assignments include serving as a Brigade S3 and a Battalion Commander in the 335th Signal Command, and Cyber Effects Chief for the 86th Training Division. Col. Erickson has three combat deployments – Iraq, Afghanistan, and Kuwait – and one overseas tour in Germany.

Cybersecurity Recommendations for Confronting the Army's Industrial Internet of Things Challenges

By Maj. Allyson Hauptman

When the 2021 attacks on the Colonial Pipeline shut down petroleum delivery for five days, it sent the U.S. into an immediate gas shortage (Beerman, 2023). Analysis of the attack showed that this incident belongs on the long list of attacks on critical infrastructures that have been made possible by negligent attitudes towards cybersecurity and poor device management processes. Recently, the U.S. has seen an evolution in attacks on critical infrastructure, where attackers have been able to exploit vulnerabilities in information technology systems to gain access to operational technologies (OT) and cause damaging and disruptive effects to the physical systems themselves (Lehto, 2022). With the pedal to the metal on updating decades-old equipment to operate in the age of the internet, the nation must consider quick and effective methods to better secure that equipment.

Graphic by Isabel S. Wences.

The Army should be heavily invested in this process for multiple reasons, including its role in Defense support of civil authorities and responsibility to various critical infrastructure sectors reliant on the U.S. Army Corps of Engineers (USACE). Here, at the Army Cyber Institute (ACI), we are spearheading research and practice for the protection of critical infrastructure with an emphasis on critical infrastructure resilience (Fontes, 2020). As we explore ways to do this, it has become apparent that the most immediate and effective way for the Army to protect critical infrastructure within its control is not some new technological innovation or complex program. Rather, it is through better cybersecurity management practices that ensure Army personnel are a part of the solution, not part of the problem.

Previous administrations have emphasized the need for a whole-of-government approach to defending critical infrastructure. The Cybersecurity and Infrastructure Agency (CISA) has defined critical infrastructure as consisting of sixteen distinct sectors (Sectors, 2020). Many of these sectors rely upon the OT found in cyber-physical systems to manage physical processes, which include industrial control systems (ICS), distributed control systems (DSC), and supervisory control and data acquisition systems (SCADA). Many of these systems have been designed to operate in an air-gapped fashion, which helps protect the systems from dangerous intrusions. SCADA systems enable remote control over industrial processes, usually over wide area networks (WANs). Over the last two decades, these networks have transitioned from being relatively isolated to more integrated with IT networks using standardized protocols, a transition being expedited by the Industrial Internet of Things (IIoT) revolution. IIoT is the transition of industrial technologies to operate with more interconnectivity, automation, and artificial intelligence (Munirathinam, 2020). While IIoT promises to ease management overhead and create more efficient, data-driven processes for critical infrastructure, it can also significantly increase the risk of exploitation and compromise to OT which did not consider cybersecurity in its design.

The IT security principles that cyber professionals learn to prioritize clash with OT priorities. In many critical infrastructure sectors, such as

energy, availability is king. Such an emphasis is understandable, as continuity of service is of paramount importance. Unfortunately, this has also created an *if it ain't broke, don't fix it* mentality that has resulted in the continued operations of systems that are either behind multiple patch cycles or still in use, despite being past their manufacturer's end-of-life (EoL) date. For a recent example, in 2021 attackers were able to gain access to the Oldsmar, Florida water treatment SCADA system by exploiting an outdated operating system (Greenberg, 2021). Patch management is often associated with downtime, and thus it is easy for operators to prioritize availability over what they think is an unnecessary patch. In practice, this means that the patches deemed necessary are the ones that address a function issue, rather than a security one. While IT networks typically plan for managed downtime, this is not true for most SCADA networks, which were built to maximize uptime. This emphasis on uptime extends to legacy systems, where a system that is no longer supported by the manufacturer but still does its job is left in place until there is a function issue. This is exemplified by the 2024 Inspector General audit of the DoD's Development and Maintenance of Digital Modernization Strategy, which found the DoD is far from meeting all four of the strategy's goals, including the employment of up-to-date systems (DODIG, 2024).

There are several reasons why these legacy systems remain in place, including the expense of replacing legacy hardware, and the fear of disrupting operations. For sectors concerned with near 100 percent availability, these may seem like legitimate reasons for delinquent patches and the use of legacy systems; however, IIoT changes the game. Security assessments generally calculate risk as the product of the likelihood and consequence of a vulnerability being exploited. Before IIoT, the likelihood of exploitation appeared small, as the devices were relatively isolated from the rest of the world. Even SCADA networks were designed to be segmented with very restricted access. As IT and OT networks integrate, and the number of devices that touch a critical infrastructure organization's network increases, the likelihood of a vulnerability being exploited increases dramatically. Reasonably, organizations are not only afraid of time to apply patches, but also that untested patches may disrupt operations, a fear fueled by the recent CrowdStrike update (George, 2024).

Organizations concerned with high availability generally err on the side of giving employees more permissions than they need, including access to management accounts. Multiple employees are given duplicative privileges in order to ensure continuity of service (i.e. if one employee is sick, on vacation, or suddenly terminated, there are immediate back-ups with all the same accesses). Multiple vulnerability assessments of critical infrastructure network systems performed by Army teams revealed that many organizations were using shared credentials with a known password, and a survey of SCADA exploits revealed default credentials to be one of the primary exploited vulnerabilities (Larkin, 2014). This is not only an access concern, but an auditing one as well, because it makes it difficult to discern the source of an intrusion.

Recent advancements in AI technologies have significantly added to the drive to build out IIoT capabilities. These IIoT solutions rely on security tools such as virtual private networks (VPNs) to ensure confidential, authorized access to the organization's network. While these tools enable increased efficiency and auditing, they also increase the number of pathways into the network for an attacker. As more employees are permitted to use these remote access tools, careful monitoring of user accounts and permissions will become increasingly difficult, as shown by their exploitation in the Colonial Pipeline case. In this case, the attacker's initial entry point into the network was through a retired employee's VPN account that did not have two-factor authentication enabled.

This example represents one type of insider threat, where the employee himself was not the threat, but the vacancy he left allowed the attacker to assume his role and access. Malicious or former employees are an even more dangerous type of insider threat. Studies show that most insider threats did not join a company with ill intent; rather, some life event encourages them to utilize the knowledge they've gained as an employee to their advantage during or post-employment. This

was the case in the cyber-attack on Five Water Utilities in 2014, where a fired engineer was able to access the station network weeks later and perform a series of malicious activities using his knowledge of the network (Hassanzadeh, 2020).

The risks of account exploitation by both outside actors and insider threats increase even further when the devices used to connect to the network are part of a Bring Your Own Device (BYOD) model. BYOD allows users to hook their potentially untested personal devices up to a network for personal or professional purposes. While BYOD has several advantages, it is incredibly dangerous for critical infrastructure, particularly if the network touches OT devices. Research has shown that one of the main attack vectors attackers pursue to reach an organization's OT is to exploit a device that intermittently connects to the business IT network. Once they gain access to the device, attackers can pivot through downstream control devices and systems. A vulnerable personal device that intermittently connects to the IT network is an ideal way to do that, as evidenced by the exploitation of a water treatment plant network in Harrisburg in 2006, where the attackers planted a virus on an employee's laptop which was later connected to the plant's internal network (Hacker, 2006).

All this to say that the IIoT revolution has turned prior sketchy, but acceptable, practices into dangerous vulnerabilities for national critical infrastructure. Furthermore, the Army faces unique challenges in confronting them. Many of these challenges are rooted in Army personnel using the same types of negligent and unsecure practices outlined above. An immediate and effective way that the Army can overcome these challenges is through the proper application of cybersecurity management practices. In this final section, I will provide three challenges and recommendations for the Army as it embraces the IIoT revolution.

Challenge 1: Guarding Against the Insider Threat

The insider threat is one the Army must be particularly concerned over due to its model of frequent job rotation. As Soldiers move between duty positions and duty locations, they gain network and facility access required to fill their new roles. Unfortunately, while organizations are encouraged to promptly get new personnel all the accesses they need to do their job, there is much less motivation to ensure that those accesses are removed once they are no longer required. This is further exacerbated by the Army's "additional duties" programs, where Soldiers are assigned additional responsibilities that are not tied to their duty position or MOS. A key aspect of minimizing a sector's vulnerabilities to these insiders is to ensure that organizations are utilizing an adequate access model that limits employee permissions to the lowest level necessary. One way to do this is through access control models that are tied to a user's assigned role, as opposed to the user themselves. A user might have more than one role, but as soon as they are removed from one of those roles, they automatically lose all privileges associated with that role.

Recommendation: The Army should require role-based access control models for all critical infrastructure networks.

Challenge 2: Securing Intermittent Devices

As IT and OT networks merge, the vulnerabilities of the IT network become vulnerabilities to the OT network, and the security of the connected devices is dependent upon the security of all the other devices. In a post-COVID world, BYOD models are no longer just about enabling personal activities. The Army has rolled out several programs to enable teleworking and distributed work, particularly for email, messaging, and file sharing. While this may be appropriate for some portions of the Army's networks, BYOD presents too many risks to unpatched, outdated, sensitive critical infrastructure systems. Many components of the Army and the DoD utilize corporate-owned models, such as Corporate Owned Business Only (COBO) and Corporate Owned Personally Enabled (COPE). In a COBO model, the business owns and strictly limits the usage of the device, and users are only permitted to use it for specific work purposes. In a COPE model, the business owns and controls the device, but users may perform limited personal activities on the device. Despite the increased IT cost for the organization, both models offer significant security advantages over a pure BYOD policy. Foremost,

because the organization owns the devices, it can incorporate them into a patch management plan, thus preventing vulnerabilities caused by unpatched operating systems and applications. Additionally, it allows the organization to whitelist the devices that are permitted to connect to specific portions of the network, helping to limit unauthorized access.

Recommendation: The Army should require the use of COBO or COPE models for critical infrastructure networks.

Challenge 3: Adding Cybersecurity to Resiliency Strategies

The DoD has numerous policies in place to enhance the resiliency of critical infrastructure, including the energy resiliency of DoD installations. The DoD is the largest consumer of energy in the United States, which has pushed it to pursue more independent, renewable energy sources with the goal of having microgrids power all military bases (Hitchens, 2024). Furthermore, the U.S. Army accounts for over one-third of the DoD's energy consumption. While installing microgrids at Army installations would enable increased energy independence and security, their deployment comes hand-in-hand with the use of IIoT technologies for remote management. Beyond generating energy, these microgrids include tertiary layers that aid in the operation and control of other critical infrastructure facilities, such as transportation, communications, waste treatment, and healthcare.

The exploitation of such a grid through an IIoT vulnerability could be catastrophic as the effects cascade along several sectors. Resiliency assessments of military microgrids have largely focused on external effects on the grid with minimal consideration and testing for cybersecurity threats (Peterson, 2021). An unfortunate reality that IIoT security must consider is that adding traditional IoT security mechanisms on top of networks connected to OT may be both ineffective and disruptive, due to the limitations of legacy devices and systems. Recent research has shown that an effective way to identify and guard against vulnerabilities in IIoT networks is to utilize security by design principles, which consider and implement controls at various stages (Mouratidis, 2018).

Recommendation: The Army should require microgrids on military installations to adhere to security-by-design principles and test those principles in resiliency assessment.

About the Author

Maj. Allyson Hauptman is a Research Scientist at the Army Cyber Institute working in the Law, Policy & Strategy Division. She holds a Ph.D. in Human-Centered Computing from Clemson University and a Master's in Cyber Security from Tallinn University of Technology. She is a Cyber Operations Officer (17A) who has served as a Mission Element Lead in the Cyber Protection Brigade and a Company Commander in the 915th Cyber Warfare Battalion (now 11th CY BN).

References

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023, May). A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 8-15). IEEE.

Department of Defense Office of the Inspector General (2024, July 9). *Audit of the DoD's Development and Maintenance of the Digital Modernization Strategy*.

Fontes, R. L., Korn, E., Fletcher, D., Hillman, J., Mitchell, E., & Whitham, S. (2020). Jack Voltaic®. *The Cyber Defense Review*, *5*(3), 45-56.

George, A. S. (2024). When trust fails: Examining systemic risk in the digital economy from the 2024 crowdstrike outage. *Partners Universal Multidisciplinary Research Journal*, *1*(2), 134-152.

Greenberg, Andy (2021, February 8). *A Hacker Tried to Poison a Florida City's Water Supply, Officials Say*. Wired. https://www.wired.com/story/oldsmar-florida-water-utility-hack/

Hacker hits Pennsylvania water system (2006, October 31). United Press International. https://www.upi.com/Top_News/2006/10/31/Hacker-hits-Pennsylvania-water-system/52641162318902/

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 03120003.

Hitchens, Kathy (2024, October 1). *Leading the Change: 3 Army Installations Launch Microgrids*. Microgrid Knowledge. https://www.microgridknowledge.com/military-microgrids/article/55166408/leading-the-charge-3-army-installations-launch-pioneering-microgrids

Larkin, R. D., Lopez Jr, J., Butts, J. W., & Grimaila, M. R. (2014). Evaluation of security solutions in the SCADA environment. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(1), 38-53.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber security: Critical infrastructure protection* (pp. 3-42). Cham: Springer International Publishing.

Mouratidis, H., & Diamantopoulou, V. (2018). A security analysis method for industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(9), 4093-4100.

Munirathinam, S. (2020). Industry 4.0: Industrial internet of things (IIOT). In *Advances in computers* (Vol. 117, No. 1, pp. 129-164). Elsevier.

Peterson, C. J., Van Bossuyt, D. L., Giachetti, R. E., & Oriti, G. (2021). Analyzing mission impact of military installations microgrid for resilience. *Systems*, *9*(3), 69.

Sectors, C. I. (2020). Critical Infrastructure Sectors. *Cybersecurity & Infrastructure Security Agency*.

OACOK, OKOCA, or OCOKA?

Reframing Terrain Analysis for Cyberspace

By Maj. JC Fernandes and Maj. Alexander Master

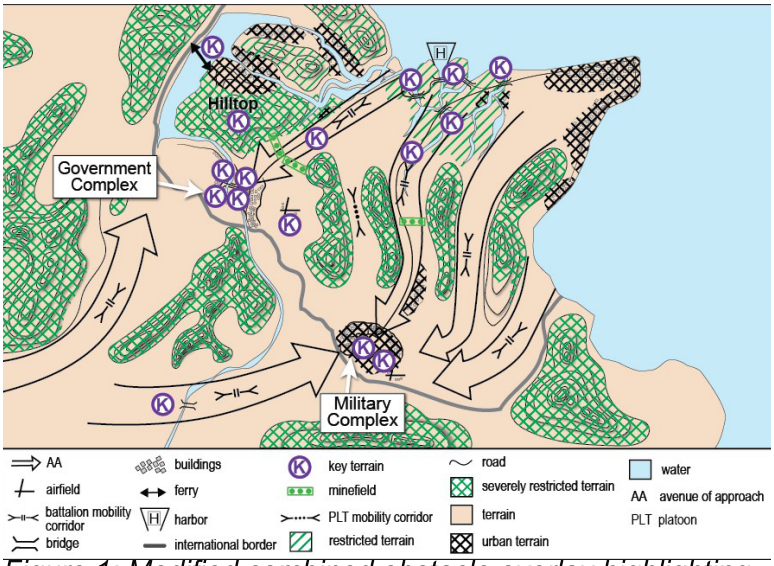


Figure 1: Modified combined obstacle overlay highlighting the key aspects of terrain analysis.

OACOK, OKOCA, or OCOKA? While they may debate the ordering, every Soldier is familiar with the mnemonic for terrain analysis. The concepts of **O**bservation and field of fire, **C**over & concealment, **A**venues of approach, **O**bstacles, and **K**ey terrain, provide a framework through which Soldiers consider the significant aspects of the terrain and their potential impacts to the operation. While OACOK is a natural starting point for Army personnel conducting cyberspace operations, the effort required to translate these land domain concepts to computer networks outweighs the convenience of the mnemonic. Cyberspace is a distinct domain of warfare with its own logic. As such, we have no assurance that elements of OACOK can serve as meaningful analogs for the operationally relevant aspect of cyberspace terrain. Instead, this paper proposes features that may be worth considering for operating in cyberspace without attempting to draw a direct comparison. The intent of this contribution is to be a conceptual linkage between military mission analysis and the robust body of cybersecurity resources (e.g., the NIST Cybersecurity Framework, the MITRE ATT&CK Framework, the Cyber Kill Chain) already available for analyzing specific aspects of cyberspace.

Why not OACOK? Unique Characteristics of Cyberspace

Before considering specific features for analysis, it is worth discussing why analysis of cyberspace is unique from terrain analysis in the land domain. Cover and concealment have a direct and personal meaning for Soldiers on the battlefield. They dictate if friendly forces can be seen and shot by the enemy, and, conversely, if they can shoot the enemy. While militaries might cut an undersea cable (Chutel, 2024) or fire artillery rounds at a key transmission node, we do not shoot kinetic munitions within cyberspace. Instead, we primarily manipulate and transmit data in very specific ways to cause effects, gain sensitive information, and defend our use of cyberspace.

The select characteristics below exemplify the unique logic of cyberspace and its unique consequences for a planner's ability to understand the aspects of the cyberspace operational environment. These characteristics are not meant to be a comprehensive description of the fifth warfighting domain but rather illuminate why we must evaluate the operational environment for cyberspace differently than we analyze physical terrain.

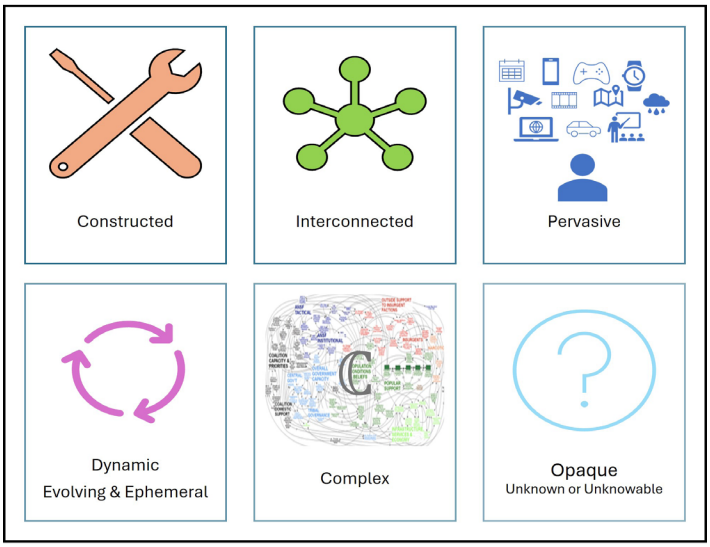


Figure 2: The unique characteristics of cyberspace

First, cyberspace is a man-made, **constructed** domain. Cyberspace comprises a multitude of software and hardware components, produced by a range of companies, organizations, and individuals across decades, and configured together in a variety of ways. This constructed nature contributes to an opaque, dynamic, and complex environment. It also blurs the distinction between terrain analysis and analysis of friendly or enemy forces. The closest military analog is dense urban environments.

Opaque: Because of overhead satellites and global imaging, Army units can generally analyze physical terrain anywhere in the world. However, like the interior of buildings, the cyberspace terrain is often opaque from the outside. Many aspects are known only to those who build and maintain that portion and their design is often confidential intellectual property. Even those who use or interact with the terrain know a limited amount about it.

Dynamic -- Ephemeral and Evolving: While mountains tend not to move and buildings do not change quickly or often, cyberspace changes at the speed of electrons. Change is often an integral part of our use of cyberspace. An IP address assignment may only be relevant for a period of hours, or less. Modern phones maintain connectivity because they can traverse cellular towers and WiFi networks. Similarly, we install new applications and create accounts for new services. Beyond usage, a patch can be pushed out and change networks across the world in a matter of minutes (e.g. CrowdStrike patch in 2024; Burgess), and hardware components are upgraded and replaced. Network diagrams are only one configuration change away from obsolescence.

Complex: Similarly, cyberspace is incredibly complex. Through abstraction, components built by many different people are combined and interoperate together without any one person understanding all the intricacies of each of the elements.

Second, cyberspace is an **interconnected** domain. Logical-layer connections between nodes define proximity in cyberspace, often in ways independent of geographic proximity. Action in one portion of cyberspace can have impacts across the globe, exponentially increasing the scope of the relevant terrain and extending it beyond the authority bounds of the unit, be it defined by geography, organizational ownership, or some other factors.

Finally, cyberspace has become increasingly **pervasive** with a subsequent increase in the diversity and scale of cyberspace terrain that may be relevant for an operation. Internet-connected devices are increasingly prolific throughout society. This pervasiveness also makes understanding the cyberspace terrain increasingly relevant to units and commanders who traditionally only need to concern themselves with the land, sea, or air domains. Because of these characteristics, cyberspace operations involve an environment whose potential scope is both extremely broad and deep, where much about the environment is unknown or unknowable.

Features for Analysis

Given the challenges of understanding the full scope of the cyberspace operational environment, we do not seek to provide an exhaustive list of items for the planner to analyze in order to understand the environment. The breadth and depth of possible analysis quickly dwarfs the staff's capacity to do so, and any exhaustive checklist would be out-of-date before it was finished being written. Likewise, content delivery networks, DNS servers, and similar facets of the domain preclude frameworks that rigidly distinguish between terrain and actors (since the domain is constructed), or rigidly define what is external to the network of interest (given its interconnected nature). Instead, we provide a list of relatively general questions – grouped into three broad thematic areas: **organizational context, network design and functioning,** and **security posture**. Just as the layout of a house may be of little consequence to someone planning a corps envelopment but is of utmost criticality when planning a raid to extract hostages, so too does the mission impact the nature and granularity of analysis appropriate for analyzing cyberspace terrain. Planners may consider these questions in the context of their mission and echelon to decide where deeper analysis is required.

Category	Items of Interest
Organizational Context	• Functions, uses, and business processes • Individual roles and privileges • Standard practices • Providers of services • Security priority
Network Design and Functioning	• Topology • Traffic flow • Hardware and software • Key network services
Security Posture	• Visibility • Tools • Measures and mitigations • Response

Figure 3: Category and analysis questions to help determine OCOKA for cyberspace.

There are many different possible names or features that could be selected, and groupings for each. However, with any grouping there are edge cases and interrelated aspects. Our concern was not that we had the perfect list of individual questions, but rather that the aggregate list would prompt the planner to consider the salient aspects for their operations and the corresponding implications.

Organizational Context:

Functions, Uses, and Business Processes: For what does the organization use cyberspace?

• What is the significance of each use? Which uses are most important? What happens if it breaks? Are there redundancies within or outside cyberspace?

• How are these functions performed? What steps, components, and individuals are involved in the different uses?

Individual Roles and Privileges: Who does what, with which authorities?

• Who has privileges for the network, content, devices, applications, etc.?

Standard Practices: What are the standard practices?

• Are there standard naming conventions for users, systems, sites, and organizational units?

• Are there standard times, locations, or people for certain tasks?

Providers of Services: How are the cyberspace capabilities provided and maintained?

• What is provided “as service” and under what conditions? (service level agreements (SLA), responsibilities)

• To what degree does change occur and what is the process for it?

• Are individuals providing their own devices (bring-your-own-device, BYOD)?

Security Priority: How is security valued by the organization and its individuals?

• Are there regulatory, legal, or other security and notification requirements?

• Has the network been compromised in the past?

Network Design and Functioning:

Topology: What are the different portions of the network, and what are they used for? (subnets/IP space, VLANs, DMZs, user space – wireless, wired, VPN)

• What is the public-facing footprint? (Across layers: applications, domains, IPs, servers, etc.)

Traffic Flow: What is the network traffic, and how does it flow?

• How does it flow between internal/public-facing servers, internal/external hosts, and the Internet?

• What is the volume, type (applications, services, protocols), and patterns (in time and direction)?

• What additional factors impact or complicate traffic? (VPN concentrators, DNS, routing rules, traffic prioritization, caching, load balancing, failover, etc.)

Hardware and Software: (host and network; public-facing and internal)

- What hardware and software are used on the network? (version, patch level, configuration)
- Where are they?
- What purpose are they used/authorized for?
- What is the process for approval, patching, and updating?

Key Network Services: What are they and how do they function?

Security Posture:

Visibility: What data is collected about traffic and endpoints and what is its lifecycle? (Collection, transmission, storage, access, removal)

Tools: What endpoint and network security solutions are present?

- What are the settings for endpoints and network traffic?
- What are the capabilities, gaps, and limitations of the implementation?

Measures and Mitigations: What technical and policy mitigations are in place?

- What system and user behavior is explicitly permitted or prohibited?
- What rules are in place for network traffic?
- How does authentication occur for users and services?
- How is data protected within the organization?

Response: How does the organization respond to alerts and incidents?

- What are the business response actions and the technical incident response actions?

These questions allow the planner to connect the broader operational context to the multitude of guides, techniques, procedures, and other resources available for analyzing specific aspects of networks and cybersecurity. In particular, the organizational context helps planners understand the significance of the cyberspace terrain and its integration with the broad joint or national context. When answering the questions, planners should consider all aspects - physical, human, and technical - holistically, rather than focusing exclusively on one domain, to ensure a more complete understanding of the implications.

Existing Frameworks and Approaches

Industry and the military offer various models that informed our selection of the above features and can complement their analysis. They provide insights into the questions we should ask, the processes we should use to ask them, and the details we should consider when answering them.

First, we proposed that cyberspace, as a complex constructed terrain with a significant human presence, is more closely analogous to a dense urban environment than wooded or rural environments. Given this premise, ASCOPE (Areas, Structures, Capabilities, Organizations, People, and Events) provides a related conceptual framework. Just as a planner cannot exhaustively analyze these elements in a large urban setting (ATP 3-06), so also do the characteristics of cyberspace preclude exhaustive analysis of the environment. However, we must view the concepts of areas and structure differently in cyberspace. Similarly, the relevant capabilities, organizations, people, and events in cyberspace may differ from those in an urban environment. Key people may include network administrators, while events may include holidays (when no one is working), but also scheduled downtime and upgrade periods.

Second, doctrine and industry also provide several common models to conceptualize cyberspace at higher levels of abstraction. JP 3-12 (OJCS, 2018) defines the interrelated layers of cyberspace – physical, logical, and person – while the Open Systems Interconnection (OSI) model (Day & Zimmerman, 1983) or the related Transmission Control Protocol/Internet Protocol (TCP/IP) model (History of Computer Communications, 2021) defines protocol layers to promote the understanding of networking. While extremely useful, the layers of these models are not features of the terrain itself but rather a lens through which to view an element of cyberspace. They are layers of abstraction that provide scope and context. While not a direct analog, they provide

similar utility to the land domain practice of analyzing terrain before, on, and after the objective. For example, in cyberspace, one might consider the physical device(s) running a web service in addition to the MAC address(es), IP address(es), and URL(s) of the server(s). Planners can consider the different layers when asking the questions proposed earlier.

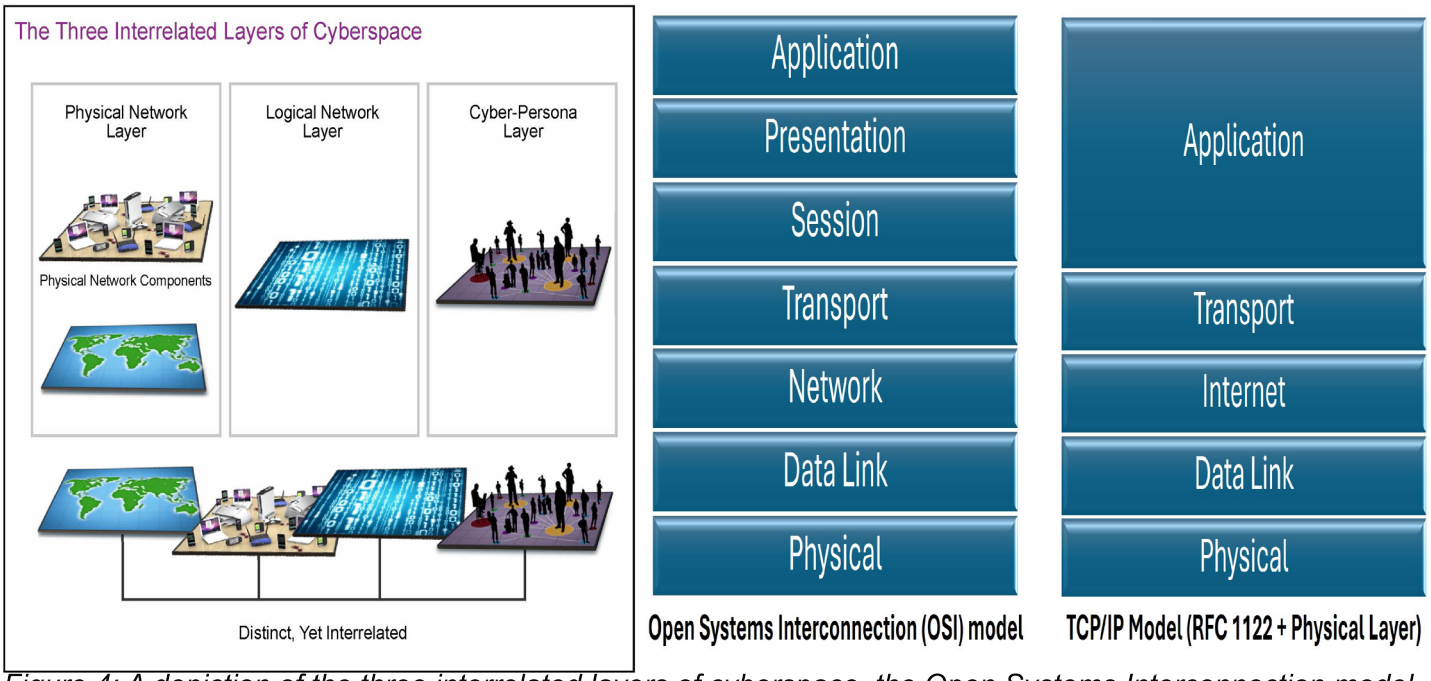


Figure 4: A depiction of the three interrelated layers of cyberspace, the Open Systems Interconnection model, and the Transmission Control Protocol/Internet Protocol.

Given the answers to questions proposed earlier, planners may determine additional analysis is required. They can turn to the rich body of cybersecurity resources from industry and government sources to dive deeper into specific aspects, such as configuration of endpoint agents, vulnerabilities of certain software, penetration testing web applications, and technical security controls.

Finally, JP 3-0 introduces the concept of a "systems perspective" for understanding the operational environment. This perspective and the related concepts of functional mission analysis (FMA), mission threads (TC 3-12.2.90), failure modes and effects analysis (FMEA), and dependency analysis, provide an approach that planners can use to focus their analysis and guide their selection of which elements to analyze.

Concluding Thoughts

We would be remiss if we failed to acknowledge that cyberspace operations do not occur in a vacuum. People use and depend on cyberspace for a variety of functions, but there can also be analog alternatives to cyberspace. The physical layer of cyberspace resides in the domains of land, sea, air, and space. It can be destroyed and impacted by power outages, extreme temperatures, electromagnetic attack, and other physical factors. The information within cyberspace is part of the information environment and can interact with the cognitive dimension as it shapes human thoughts and behaviors - which may have subsequent impacts on users' activities in cyberspace. To conduct joint, multi-domain operations that achieve synchronized effects in time and space, cyber planners must not only understand the cyberspace terrain but also how it fits into the broader operational environment and operational objectives. The organizational context provides planners with the means to do just that.

About the authors

Maj. JC Fernandes is an active duty Cyber Officer at the Army Cyber Institute. He conducted defensive cyber operations while assigned to the Cyber Protection Brigade. He was initially commissioned as an infantry officer and served with the 173rd IBCT(A).

Maj. Alexander Master is an active duty Cyber Officer at the Army Cyber Institute and an Assistant Professor in the Electrical Engineering and Computer Science department at the United States Military Academy at West Point, New York. His research interests focus on digital privacy and force protection. Maj. Master has served on a National Cyber Protection Team, and spent three years supporting offensive cyberspace operations in the Cyber National Mission Force. He was initially commissioned as a field artillery officer and deployed in support of Operation Resolute Support in 2015 as part of the conflict in Afghanistan

References:

Burgess, M. (2024). Microsoft outage caused by CrowdStrike takes down computers around the world. WIRED. https://www.wired.com/story/microsoft-windows-outage-crowdstrike-global-it-probems/

Chutel, L. (2024). Finland Says Vessel Suspected of Cutting Cable May Be Part of Russia's 'Shadow Fleet'. The New York Times. https://www.nytimes.com/2024/12/26/world/europe/finland-estonia-cables-russia.html

Day, J. D., & Zimmermann, H. (1983). The OSI reference model. *Proceedings of the IEEE, 71*(12), 1334–1340. https://doi.org/10.1109/PROC.1983.12775

History of Computer Communications. (2021). The Department of Defense, OSI, and TCP/IP. https://historyofcomputercommunications.info/section/14.5/The-Department-of-Defense-OSI-and-TCP-IP/

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2018). MITRE ATT&CK: Design and philosophy. MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Lockheed Martin. (2011). Cyber kill chain. Lockheed Martin Corporation. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Office of the Joint Chiefs of Staff. (2018). Joint publication 3-12: Cyberspace operations. U.S. Department of Defense. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

OWASP. (2025). The OWASP Risk Assessment Framework. Open Worldwide Application Security Project (OWASP). https://owasp.org/

Ullrich, S., & Moriarty, S. (2024). Lessons learned from the Ukrainian Territorial Defense Forces: Command post survivability. United States Army. https://www.army.mil/article/273510/lessons_learned_from_the_ukrainian_territorial_defense_forces_command_post_survivability

U.S. Army. (2022). ATP 3-06: Urban Operations. U.S. Department of the Army. https://armypubs.army.mil/ProductMaps/PubForm/ATP.aspx

U.S. Army. (2024). TC 3-12.2.90 Mission Thread Defense. U.S. Department of the Army. https://armypubs.army.mil/ProductMaps/PubForm/TC.aspx

The Value of 1,000 Papercuts: A Paradigm Shift in the Strategic Environment

By Lt. Col. Luis "Lou" Etienne Jr.

The book "Cyber Persistence Theory" by Michael Fischerkeller, Emily Goldman, and Richard Harknett suggests a paradigm shift of the strategic environment shaped by the Cold War and twenty years of fighting the Global War on Terrorism. Cyber Persistence Theory recognizes that cyberspace, the only manmade warfighting domain, adds a level of complexity to the strategic environment that cannot be fully conceptualized using the security paradigms shaped by Coercion Theory.[1] Coercion is the ability to get an actor – a state, the leader of a state, a terrorist group, a transnational or international organization, or a private actor – to do something it does not want to do.[2] Dr. Tami Biddle, author and distinguished fellow at the U.S. Army War College, states the following, "Coercion is about future pain, about structuring the enemy's incentives so that he behaves in a particular way. It manipulates the power to hurt and involves making a threat to do something that has not yet been done."[3] The terms "hurt" and "pain" reveal a vital nuance in Coercion Theory. An opponent cannot be deterred from an action or compelled to take an action if they do not understand the "hurt" and "pain" that comes with deciding on the alternative. The traditional interpretation of "hurt" and "pain" as it applies to coercion is why some from the academic and policy communities take issue with the term "cyber war". Thomas Rid, the director of the Alperovitch Institute for Cybersecurity Studies and a professor of Strategic Studies at Johns Hopkins University, argues that cyber war has not and will not occur. He believes no cyber-attack will meet Clausewitz's criteria of war - that it must be violent, instrumental, and political.[4] Instead, he categorizes cyber-attacks as either sabotage, espionage, or subversion.[5] Erik Gartzke, a Professor of Political Science at the University of California San Diego, argues that "cyber-attacks have not transformed states pursuit of strategic advantage." He claims that cyber operations can only be relevant in grand strategic terms if they accomplish the following tasks related to military violence in the physical domains: deterring and compelling, maintaining or altering power distribution, and resisting or imposing disputed outcomes.[6] In other words, cyber effects must coerce an actor to take or not to take an action. Like Rid, Gartzke believes that the criterion for war in the traditional sense has not been met. Rid and Gartzke's assertions demonstrate the complexity of using Coercion Theory to explain the impact cyber operations can have towards strategic objectives. The subtleties that the cyber domain presents to the strategic environment require its refinement of the models used for international relations. Failure to understand the paradigm shift will lead to an inability to measure the effectiveness of operations in cyberspace.

Cyber Persistence Theory suggests a paradigm shift where "cyberspace must be understood primarily as an environment of exploitation rather than coercion. Achieving strategic gains in the cyber strategic environment does not require concession of the opponent." Cyber Persistence Theory posits that an actor can reset the cyber playing field without shaping the decision calculus of an opponent, and thus states must "anticipate the persistent resetting of security conditions in cyberspace by others and seek to do so in return."[7] Albeit just a theory, current events in the global landscape serve as evidence that state actors are already applying concepts from Cyber Persistence Theory to further their strategic objectives. This paper will examine the recent Chinese response to Speaker Nancy Pelosi's visit to Taiwan and the U.S. response to Russian interference in the 2016 presidential election to illustrate how major powers are realizing the shift in the security paradigm driven by the nascent cyberspace domain. It will further demonstrate how China and the U.S. are applying concepts of Cyber Persistence Theory to gain advantages in the strategic and information environment.

On August 2, 2022, House Speaker Nancy Pelosi landed in Taipei, Taiwan for an official visit. Her visit marked the first time a House Speaker visited Taiwan in 25 years.[8] The Chinese Communist Party (CCP) saw Speaker Pelosi's visit to Taiwan as an act of contention, further igniting the already volatile China-Taiwan Cross Strait rela-

tions. In response to the visit, the People's Republic of China (PRC) suspended talks with the U.S., communicated threats and warnings to the international community regarding interfering with "sovereign matters", and conducted large scale military exercises in the Taiwan Straits. These exercises included firing missiles over Taiwan that landed right outside Taiwan controlled waters.[9] These coercive responses indicate that the CCP still see value in operating within the traditional coercion-based security paradigm. Although extremely measured, the military exercises and firing munitions close to Taiwan owned waters are actions meant to demonstrate the pain China can impose on Taiwan. Whether or not these actions effectively deter further U.S.-Taiwan diplomatic engagements, they do allow for the U.S. and Taiwan to clearly calculate the costs of continuing to disrupt the status quo of the cross-strait relations.

However, the traditional coercive responses orchestrated by the CCP were not the only responses observed before, during, or after Speaker Pelosi's visit to Taiwan. There was also an observation of actions taken in cyberspace and the information environment. Taiwan's Digital Minister, Audrey Tang, reported that the volume of cyber-attacks against Taiwan on the day Speaker Pelosi's visit was approximately twenty-three times the previous single-day record. The website for the Office of the President, the Foreign Ministry, the Defense Ministry, and the Taoyuan International Airport – the largest in Taiwan – were brought down by a distributed denial of service (DDOS) attack. Display screens at railway stations were also hacked to display protest messages against Speaker Pelosi's visit.[10] 7-Eleven stores in Taiwan reported that their store televisions were hacked to display the message "Warmonger Pelosi, get out of Taiwan," and that one of the affected stores was a 7-eleven Speaker Pelosi visited during her trip. 7-Eleven is the largest convenience store chain in Taiwan.[11] Moreover, the day Speaker Pelosi departed Taiwan, a false-flag Chinese hacktivist group named APT27_Attack declared "cyberwar" against Taiwan's government and commercial organizations. They conducted what Trellix, a cybersecurity company, called special cyber operations against Taiwan for five days. The target of their attacks were the government offices, train stations, convenience stores, and the retail and manufacturing conglomerate, Uni-President.[12] The strategic impact of these responses in the cyber and information domain were undoubtedly minimal. However, international news mediums widely covered the aforementioned actions. These cyber and information operations demonstrated the ability to amplify traditional military and diplomatic coercion through actions taken to manipulate and control elements of the cyber strategic environment. Outside the self-admittance of actions by the APT27_Attack Chinese hacktivist group, there has been no attribution for the response actions taken in the cyber and information realm after Speaker Pelosi's visit to Taiwan.[13] However, one can assume that the Chinese either orchestrated or supported these response actions. The mere fact is that the CCP did not condemn the attacks in cyberspace and the information environment is telling. Regardless, the response actions to Speaker Pelosi's visit in the cyber domain and information environment address aspects of the strategic environment that are not addressed solely by traditional coercive means. The CCP recognized an opportunity to gain an understanding on actions in cyberspace and the information environment that impact the decision calculus of the U.S. and Taiwan. The CCP overt response actions to Speaker Pelosi's visit clearly show that it still looks to shape the strategic environment using the more traditional, coercion-focused security paradigm. It is likely that the CCP also played a role in the cyber and information related responses to Speaker Pelosi's visit as well, which would demonstrate their recognition of a shift in the security paradigm and the CCP's desire to gain the advantage in the contemporary cyber strategic environment.

The response to the Russian Federation's interference in the 2016 election, and the 2018 Department of Defense Cyber Strategy's concept of defending forward, serve as evidence that the U.S. recognizes a shift in the security paradigm. In 2018, U.S. Cyber Command (USCYBERCOM) conducted an operation to block internet access to the Internet Research Agency, a Russian troll factory, to deter Russian cyber operations from disrupting the 2018 midterm elections. To prevent Russian hacktivist and proxy hackers from conducting operations in support of Russia's

interference campaign, USCYBERCOM also sent direct messages to Russian hackers revealing that the U.S. knew their identities. Additionally, in response to reported Russian cyber operations against U.S. critical infrastructure, USCYBERCOM prepositioned an implant on Russian energy infrastructure, with the intent of signaling the cost of Russian continued attempts to access U.S. critical infrastructure.[14] The U.S. government and military's predominant use of cyber operations in response to Russian interference with U.S. elections demonstrated their understanding of a paradigm shift in the strategic environment. The Russian threat in 2016 was not one of a destructive force that put the lives of U.S. citizens at risk; it was a threat to the legitimacy of the election process that assures free and fair elections in the U.S. The Russian disinformation campaign was delivered through cyberspace and the information environment. As dangerous as this threat was to American foundational narratives and values, it did not warrant a kinetic response. The Russians were posing a different type of threat in an ill-defined cyber strategic environment. The actions of the Russian Federation during the 2016 presidential elections forced the U.S. government to recognize the new security paradigm. The U.S. understood that responding to the contemporary threat posed by Russia would take an understanding of the contemporary cyber strategic environment.

Adversarial activity in cyberspace like the Russian election interference in 2016, shaped the content of the 2018 Department of Defense (DoD) Cyber Strategy. The strategy calls for the United States to defend forward "to disrupt malicious cyber activity at its source, including activity that falls below the level of armed conflict." The responsibility for defending forward starts with USCYBERCOM and the concept is a shift in approach to the security of critical networks, critical infrastructure, and key resources of the U.S. With this strategy, the DoD's posture for defending in cyberspace shifts from reactive to proactive. The concept of persistent engagement against malicious cyber actors (MCAs) guided the development of the strategy's operational framework. Under this operational framework, USCYBERCOM commits resources and capabilities daily to "intercept and halt cyber threats, degrade adversary capabilities and networks, and continuously strengthen the cybersecurity of the Department of Defense Information Network (DoDIN) that supports DoD missions."[15] To persistently engage in cyberspace, USCYBERCOM must not only be ready to respond in kind to malicious cyber activity against U.S. critical networks, critical infrastructure, and key resources, but it must also be ready to preemptively take the proverbial fight to the adversary outside defended cyberspace. To achieve the strategy's objectives, leaders in the DoD, engaging daily in grey (neutral third-party) and red (enemy) cyberspace, require the delegation of offensive cyber authorities to allow for faster and more agile decision-making. The Trump administration addressed this policy by publishing the National Security Presidential Memorandum 13 (NSPM-13). NSPM-13 is a classified document, so the details are not public.[16] However, Brigadier General Alexus Grynkewich, the deputy for global operations on the Joint Staff from June 2017 to April 2019, provided a general overview of the policy. Brig. Gen. Grynkewich stated that NSPM-13 "provides a way, within certain policy constraints, for the president to delegate cyberspace authorities to the secretary of defense for a particular mission."[17] NSPM-13 essentially affords the DoD the ability to be more agile in their decision making by removing bureaucratic distractions from the approval process for executing offensive operations in cyberspace. These policy shifts fundamentally change the way that the U.S. government and DoD approach problems in the cyber strategic environment.[18] The proactive language of the DoD Cyber Strategy and the leeway granted to the DoD to conduct cyber operations in spaces that were mostly off-limits in the past, demonstrate the government's commitment to the concept of defending forward and persistent engagement. The 2018 DoD Cyber Strategy and NSPM-13 along with the U.S. government response to Russian election interference in 2016 also demonstrate that the U.S. government recognizes that cost imposition in the cyber strategic environment requires a different approach than the traditional coercive approach of threating violence or destruction.

Major powers in the current world order are making efforts to gain a decisive advantage in cyberspace and the information environment.

Cyber Persistence Theory posits that the advantage goes to the entity that adopts the shift in the security paradigm and looks at the effects of cyber operations for what it is. Until cyber-attacks demonstrate the ability to cause "pain" or "hurt" in the same manner that a nuclear attack does, coercion of an opponent by means of cyber-attack will continue to be a misnomer.

However, pain and hurt have levels, and an opponent will feel all levels of pain and hurt in some way. If a nuclear attack is a gunshot and a cyber-attack is a paper cut, then death by a thousand paper cuts is the only way to coerce an opponent with cyber-attacks. Cyber Persistence Theory offers that there is value in inflicting 100, 200, or 500 paper-cuts, and suggests that actors must find a way to understand this value in the cyber strategic environment.

About the author

Lieutenant Colonel Luis (Lou) Etienne graduated from the United States Military Academy in 2004 and commissioned as an Infantry Officer. In 2012, Lt. Col. Etienne was assigned to 704th Military Intelligence Brigade where he served as a Senior Collection and Execution Officer and Deputy Division Chief of the Collection Pursuit Division in the NSA/CSS Threat Operations Center. In 2015 Lt. Col. Etienne transitioned into the Cyber branch, where he has held several leadership roles including Mission Team Lead for 401 Cyber Protection Team, Executive Officer of 2nd Cyber Protection Battalion, Executive Officer of 915th Cyber Warfare Battalion, Mission Team Lead for 01 National - Cyber Protection Team, and Deputy Commander of Joint Task Force-2, Cyber National Mission Force. Lt. Col Etienne is currently the commander of the 11th Cyber Battalion, the Army's only expeditionary CEMA battalion.

Endnotes

1 Michael Fischerkeller, Emily Goldman, and Richard Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022), 1.

2 Robert Art and Kelly Greenhill, "Coercion: An Analytical Overview," in *Coercion: The Power to Hurt in International Politics*, ed. Kelly Greenhill and Peter Krause (New York: Oxford University Press, 2018), 5.

3 Tami Davis Biddle, "Coercion Theory: A Basic Introduction for Practitioners," The Strategist, Texas National Security Review, 3, no. 2 (2020): 16.

4 "Trid2," Johns Hopkins SAIS, accessed December 14, 2022, https://sais.jhu.edu/users/trid2.

5 Fischerkeller et al, *Cyber Persistence Theory*, 4.

6 Ibid, 4-5.

7 Ibid, 1.

8 Nectar Gan et al., "Taiwan: What to Know about Nancy Pelosi's Visit," CNN, August 3, 2022, https://www.cnn.com/2022/07/29/asia/pelosi-taiwan-visit-explainer-intl-hnk/index.html.

9 Erica Lonergan and Grace Mueller, "What Are the Implications of the Cyber Dimension of the China-Taiwan Crisis?," Council on Foreign Relations, August 15, 2022, https://www.cfr.org/blog/what-are-implications-cyber-dimension-china-taiwan-crisis.

10 Sarah Wu and Eduardo Baptista, “From 7-11s to Train Stations, Cyber Attacks Plague Taiwan Over Pelosi Visit,” Reuters, August 4, 2022, https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/.

11 Matthew Loh, “Some of Taiwan’s 7-Eleven Outlets Said an ‘unknown Source’ Hacked Their Store TVs to Display the Message ‘Warmonger Pelosi Get out of Taiwan,’” Business Insider, August 3, 2022, https://www.businessinsider.com/taiwan-nancy-pelosi-7-11-hack-get-out-messages-cyberattack-2022-8.

12 Anne An, “Cyber Tools and Foreign Policy: A False Flag Chinese ‘APT’ and Nancy Pelosi’s Visit to Taiwan,” Trellix: Stories, September 29, 2022, https://www.trellix.com/en-us/about/newsroom/stories/research/cyber-tools-and-foreign-policy.html.

13 Wu and Baptista, “From 7-11s to Train Stations”.

14 Joe Devanny, “‘Madman Theory’ or ‘Persistent Engagement’? The Coherence of US Cyber Strategy under Trump,” Journal of Applied Security Research 17, no. 3 (July 3, 2022): 282–309, https://doi.org/10.1080/19361610.2021.1872359.

15 USCYBERCOM PAO, “CYBER101 - Defend Forward and Persistent Engagement,” U.S. Cyber Command, October 25, 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber101-defend-forward-and-persistent-engagement/.

16 Herb Lin, “President Biden’s Policy Changes for Offensive Cyber Operations,” Lawfare (blog), May 17, 2022, https://www.lawfareblog.com/president-bidens-policy-changes-offensive-cyber-operations.

17 Sydney Freedberg, “Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff,” Breaking Defense (blog), September 17, 2018, https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/.

18 Ibid.

Cyber Joint Inter-Agency Task Forces

By Maj. Geoffrey Crawford

How do leaders identify the best cyber capability to achieve an objective? Once identified, how do they quickly and effectively bring the chosen capability to bear? In the current environment, the Army relies on limited Liaison Officer (LNO) relationships, which have long lead times, to access the capability. If the capability or terrain requires interagency support, interpersonal relationships and processes must be established on an ad-hoc basis; however, these relationships typically dissipate once the mission is completed. Operations in the cyber domain are complex, with no geographic limitations on friendly or adversary maneuver. A regional power with limited power projection capabilities, such as Iran or North Korea, can operate at scale in cyberspace; this complicates the requirements placed on regional combatant commands and has an outsized potential of hindering unity of effort when facing nation-states. The United States Central Command (USCENTCOM) Commander will inevitably view and engage Iranian cyber threats differently than the United States Indo-Pacific Command (USINDOPACOM) Commander, and vice versa for North Korean cyber threats. This problem extends outside Department of Defense (DOD) entities, with the National Security Agency (NSA) and CIA approaching cyber threat actors and nation-states differently than DOD forces. There are many stakeholders operating within the cyber domain, including the FBI, NSA, CIA, and DOD. All these stakeholders have their own approaches, goals, and priorities. These differences create an expansive menu of capabilities for national and strategic leaders but make deconfliction and synchronization difficult. The problem facing the DOD and all United States cyber stakeholders is to present a unified force that can operate both synchronously and asynchronously, while deconflicting operations to achieve unity of effort, increasing responsiveness to national and strategic level needs, and preserving freedom of operations. The solution will likely require one or multiple cyber centers of gravity, which would serve as a “one-stop shop” for leaders to find or create the correct capability to quickly and efficiently meet requirements.

Joint Task Force ceremony depicting various branches of services working together. (Photo by Petty Officer 1st Class Samantha Jetzer

U.S. national and strategic level leaders face an uphill battle to coordinate and win in cyberspace. The domain and threat landscape constantly change at a speed that does not allow long decision cycles. It is complex, with threats coming from criminals, nation-states, protest groups, and anyone with malicious intent and access to the internet. It is global and requires a high degree of coordination to achieve valuable effects. The capabilities that those leaders can leverage are often disjointed, with little unity in effort or command, and each stakeholder has divergent priorities and objectives. All of this culminates in a domain that is fraught with challenges, which are becoming increasingly vital to navigate in order to operate effectively on the world stage. The centers of gravity would need strong habitual linkages to all stakeholders and the ability to make decisions and allocate resources in order to answer these challenges. By having a center of gravity with these linkages, situational understanding will increase and allow for a single panel of glass for leaders. This will also allow for better information and resource sharing, improving cyber forces’ posture and reducing unnecessary redundancies.

The one-stop shop approach will increase the interconnectedness of stakeholders and allow them to engage threat actors more effectively through a “whole of” government approach. The list of threat actors’ objectives and tactics, tech-

niques, and procedures are varied. New threats present themselves almost daily in cyberspace. Some criminal actors operate for profit and do not directly correlate to U.S. priorities. They can easily hold cyber assets at risk or sell access to nation-state actors. This creates complexity and difficulty in adequately prioritizing defensive assets and creates challenges for keeping pace with a threat landscape that is constantly changing.

Proposed Solution

A solution is the creation of Joint InterAgency Task Forces (JIATFs) that can either be threat or regionally aligned. The Joint Interagency Coordination Group Core Element would consist primarily of NSA and DOD personnel with LNOs, Memorandum of Understandings (MOUs)/Memorandum of Agreements (MOAs), and augmentation from other stakeholders on a permanent, semi-permanent, or as-needed basis. The JIATF would answer to the United States Cyber Command (USCYBERCOM) commander through NSA and USCYBERCOM staffs to answer Secretary of Defense (SECDEF), Combatant Commanders, and State Department requirements. The DOD bill payers to build this organization would be the Joint Force Headquarters-Cyber (JFHQ-C). Like JFHQ-Cs, the JIATF would have operational control of DOD cyber teams and operational control of NSA assets that align with the JIAFT's focus area. The JIATF would operate like an Air Operations Center by deconflicting operations in cyberspace, building mission/target packages, conducting cyber mission planning, and being the primary bridge between the Combatant Commander (CCMD) and cyber forces.

The joint approach has been used to address similar challenges in other areas of the DOD. JIATF-South was established to counter drug trafficking using all-domain capabilities through interagency collaboration and partnering with nations to target, detect, and monitor illicit drug trafficking in the air and maritime domains. They use this collaboration to leverage different authorities, relationships, and intelligence streams to magnify each agency's strengths and increase JIATF-South's effectiveness. Since its inception, JIATF-South has helped to interdict over 100 tons of cocaine annually, which represents approximately 60% of the U.S. Government's successful maritime drug interdictions. The National Cyber Investigative Joint Task Force (NCIJTF) was established in 2008 by National Security Presidential Directive 54, with the primary responsibility of developing and sharing information related to cyber threat investigations across the cyber stakeholder community, while coordinating and integrating associated operational activities to counter adversary based cyber threats. One of the current projects for NCIJTF is developing a capability to maintain awareness of federal computer intrusion investigations and help link cases across agencies. NCIJTF has fostered increased collaboration and uses its members' collective authorities and capabilities to bring available resources to bear against domestic cyber threats. In 2021, NCIJTF was instrumental in coordinating FBI, NSA, and Department of Justice (DOJ) support to operations against the REvil ransomware group; this ultimately led to the seizure of cryptocurrency payments and disruption of the group's infrastructure. These joint interagency formations have increased cooperation and integration while allowing for a whole-government approach to a specific problem set. They leverage relationships and synergy to achieve objectives that none of their components could achieve individually.

Mission and Goals

The mission of the cyber JIATFs would be to plan, synchronize, and coordinate across the cyber domain inside their area of operations and increase access and responsiveness for all capabilities and assets. They will also provide improved shared situational awareness for the entire cyber force, as well as senior leaders. The goal of the JIATFs is to provide responsive and adaptable support to answer regional, strategic, and national priorities; the joint forces will also combat emerging threats in the cyber domain through unity of effort across the whole of government.

In practice, cyber JIATFs would allow Combatant Commanders to have a single point for requesting support and understanding the cyber battlespace in their area of operations. JIATFs can provide subject matter expertise for regional cyber efforts and focal points for emerging threats in their areas of focus. JIATFs would be able to

coordinate amongst themselves to ensure commonality across approaches and engagement with nation-states operating in cyberspace. As an example, a JIATF would help ensure that USINDOPACOM's and USCENTCOM's responses to North Korean cyber actors are synchronized and the best capability or asset is being leveraged. Additionally, the JIATF can create synergy for cyber forces during operations. Instead of a cyber team having to answer Combatant Commander, JFHQ-C, and USCYBERCOM priorities simultaneously, the team can focus on supporting the JIATF's priorities and allow the JIATF, with its staff, to engage outside entities. This focuses the team on the mission instead of navigating different stakeholders' priorities and staff power dynamics.

The cyber JIATF approach to this problem set produces an interesting use case for the Department of Defense Information Network (DODIN). JFHQ-C DODIN is responsible for protecting the Defense Information System Agency's (DISA) infrastructure. JFHQ-C DODIN is not responsible for securing subcomponents of the DODIN, such as DODIN-Army. United States Army Cyber Command (ARCYBER) protects DODIN-Army, and the other services are responsible for their own subcomponents of the DODIN. This creates differing responsiveness to threats and no easy way to coordinate defensive efforts across the subcomponents of the DODIN. Establishing a JIATF-DODIN with responsibilities to operate across the entire DODIN with teams from across the DOD would improve and standardize responses to threats while increasing information sharing for emerging and ongoing response actions. This would enable improved whole-of-government approaches to threats against critical infrastructure. Since JIATF-DODIN would already be strongly integrated with FBI, Homeland Security, and Department of Justice, it would reduce the lead associated with creating a task force to address a crisis. JIATF-DODIN would provide a standardized defense of the U.S. cyber footprint. This would also allow for better use of all authorities to conduct investigations and pursue criminal prosecution when necessary.

Adversary and Ally Approaches

China has already created a whole government approach to cyber domain building, which amounts to a centralized cyber strategy. They focus heavily on commercial and government integration. China actively leverages companies like Huawei and Tencent to conduct cyber espionage and improve their use of technology. The government has bolstered integration through laws, like the National Intelligence Law of 2017, to ensure synergy across all sectors for cyber operations. They use a highly centralized framework with the People's Liberation Army Strategic Support Force (PLASSF) integrating cyber, electromagnetic, and space capabilities to achieve offensive and defensive effects. This deeply integrated approach allows for faster decision-making and easy access to many capabilities. In the current U.S. construct, though the U.S. can achieve similar integration of capabilities, this integration would be slowed by the need to stand up as an ad hoc organization.

Though less centralized, the Russian approach uses many non-state actors and cybercriminal groups to achieve state objectives. They have demonstrated a homogenous approach to using the cyber domain to achieve national objectives like disinformation and destabilizing infrastructure. They attack government and civilian systems to accomplish these objectives through hybrid operations. The U.S. can counter these tactics and improve detection and responsiveness by focusing on better interagency coordination.

The European Union has established the European Union Agency for Cybersecurity (ENISA), which coordinates cybersecurity efforts across member states, focusing on threat intelligence sharing. They have also established the Cyber Crisis Liaison Organization Network (CyCLONe) to facilitate coordination during cyber crises among national Computer Security Incident Response Teams (CSIRTs). These organizations bolster coordination and cooperation to disrupt threat actors and reduce the effectiveness of any threat actor's operation.

The United Kingdom has established the National Cyber Security Centre (NCSC) as part of the Government Communications Headquarters (GCHQ). The NCSC provides a centralized hub for managing cyber incidents, sharing threat

intelligence, and advising public and private sectors during cyber-attacks. The NCSC was instrumental in the UK's response to the WannaCry ransomware attack. The UK also has the National Offensive Cyber Programme (NOCP), which integrates military and intelligence agencies to conduct offensive cyber operations against adversaries.

Many allies and adversaries have identified the need for close cooperation and integration across stakeholders operating in the cyber domain and have established organizations to achieve this effect. These organizations have proven to be enablers that support faster responses, reducing threat actors' effectiveness by allowing cyber forces to be brought to bear more rapidly.

Conclusion

U.S. cyber stakeholders must provide elite capabilities to national and strategic leaders that will enable rapid offensive and defensive actions while providing an easy-to-digest menu of options for those leaders. To combat the increasing attack surface and growing threat in the cyber domain, stakeholders must be able to respond quickly and in coordination with other stakeholders. Historically, this has been ad hoc and only when a need arises, but that lengthens response time and requires a long lead time to facilitate. The decision-making space in cyber is getting shorter, so senior leaders need a fast and reliable way to understand the cyber domain and where friendly forces are operating. Cyberspace requires a whole-of-government approach because of its interconnectedness. Both ally and adversary nations have begun to increase integration among cyber stakeholders, increasing demand for the U.S. to keep pace. The JIATF approach can reduce lead time, reduce redundancy, improve responsiveness, and multiply the effects for stakeholders.

About the author

Maj. Geoffrey Crawford is an an instructor for Cyber Warfare Officer Basic Officer Leaders Course (CWO-BOLC) in the Cyber Training Battalion (CTB). Prior to serving in the CTB, Maj. Crawford attended resident Command and General Staff College (CGSC) at Fort Leavenworth, KS. Before CGSC, he was assigned to the Cyber Protection BDE, where he held positions as a Cyber Protection Team (CPT) Team Lead, battalion S-1, and Mission Element Lead. Maj. Crawford served as a Team Lead for 503 CPT, which supported USINDOPACOM and the Team Lead for 156 CPT, an Army service team focused on Industrial Control Systems technology. He was the Mission Element 1 lead for 91 CPT, which is the only Army team that supports the DoD Information Network (DoDIN).

Bridging the Cyber Divide: Common Ground in Cyber Operations

By Maj. John Plaziak

Four countries, thirty-seven attacks, and thousands of lives lost. This was the devastating toll of the Islamic State in Iraq and Syria's (ISIS) global campaign of terror following their 2014 capture of Mosul, Iraq's second-largest city. As the extremist group transformed the ancient metropolis into their self-proclaimed capital, they unleashed a wave of violence that would soon force military strategists to reimagine modern warfare.

Online propaganda ran rampant. ISIS, through the Cyber Caliphate, began recruiting and messaging their cause through social media and dark web forums. Military operations needed to expand from the physical into the digital realm. The increasing cyber threat led to the formation of Joint Task Force ARES, a unit within U.S. Cyber Command, tasked with conducting Operation Glowing Symphony in 2016.

The mission aimed to disrupt ISIS's digital infrastructure by infiltrating and compromising its media networks. Cyber operatives targeted ISIS's servers, websites, and social media accounts, effectively impeding their ability to spread propaganda and coordinate activities. This cyber offensive significantly degraded ISIS's online presence, hindering its recruitment efforts and operational planning.

Operation Glowing Symphony marked a pivotal shift in modern warfare, highlighting the importance of cyber operations in combating extremist groups. By targeting the digital platforms that facilitated ISIS's growth, the operation showcased the potential of cyber strategies to undermine the capabilities of such organizations.[1]

Analysis of OGS Through Strategy

A significant theme throughout OGS is the herculean task of understanding the parts and interconnected nature of the ISIS media network. Through Joint Intelligence Preparation of the Operational Environment, USCYBERCOM teams could "map out" this network of people, places,

Maj. John Plaziak, U.S. Army Command General Staff College

physical infrastructure, logical links, and information.

The resulting web of information seemed complex. The cause-and-effect analysis placed on different parts of the network map was difficult to understand, thus making it difficult to prescribe action against them. However, through careful analysis, a captain on a cyber mission team was able to identify patterns in the network map. Through these patterns, he began center of gravity analysis, an analysis of the source of strengths of the ISIS media network. He discovered critical capabilities, critical requirements, and critical vulnerabilities of the ISIS media network (Joint Staff, 2024, pp. IV-22 to IV-27). These critical vulnerabilities could be targeted to have a measured effect. He conducted intellectual bracketing by using a combination of intuition and cognition with the data, information, and knowledge available to him, resulting in a deeper understanding of his problem (McConnell, Mong, & Ptaschek, 2021). The ISIS media network was, in fact, a complicated system rather than a complex one. Joint Task

Force Ares was created to conduct the operation against these identified vulnerabilities.

Analysis of OGS Through Tactics

Defeat mechanisms are essential in describing the desired effect of an offensive operation. Of the four mechanisms—destroy, dislocate, disintegrate, and isolate—OGS displayed qualities associated with destruction and disintegration (HQDA, 2022, pp. 3-20). It is conceivable that offensive cyberspace operations could support any defeat mechanism. Leaders across formations and branches must communicate their expectations in this common language to accomplish the commander's intent.

In a traditional offensive operation, combat force ratios favor the defender, giving them a relative advantage (HQDA, 2023, p. 8-24). In cyberspace, however, this favor is reversed. In the military and industry, cyber defenders struggle to maintain the defensive posture required to keep an adversary out of their systems and networks. Due to the relatively low cost of an attack, as opposed to a traditional military offensive operation, an offensive cyber operation only needs to be successful once. The defender, however, must be successful every time. This concept flips the traditional framework that military planners use and should be accounted for when considering offensive and defensive operations in cyberspace. OGS planners could then use this analysis when planning and executing their mission.

Analysis of OGS Through Force Management

The Joint Capabilities Integration and Development System (JCIDS), a Department of Defense (DoD) process for identifying capability requirements and validating solutions, can be used literally and metaphorically during Operation Glowing Symphony (USAWC, 2021, pp. 2-14).

From a metaphorical perspective, the Department of Defense identified a critical gap in its plan to defeat ISIS. This gap led to a cyberspace line of effort aimed at combating the Cyber Caliphate and its associated media networks. Operation Glowing Symphony was born through this identified and filled capability gap.

From a literal perspective, JCIDS represents the mechanisms for leaders to identify gaps in the current cyber capability set through the Doctrine, Organization, Training, Material, Leadership and Education, Personnel, and Facilities (DOTMLPF) lenses. Once the gaps are identified, the force management system could create the appropriate material or non-material solution.

Analysis of OGS Through Sustainment

Sustainment provides three things to a commander: operational reach, freedom of action, and prolonged endurance (U.S. Joint Chiefs of Staff, 2023, p. III-26). While sustainment in the traditional sense provides resources to continue the fight in an area of operations, cyberspace operations typically defy those requirements due to their non-theater requirements, as depicted during OGS. However, operational contract support and finance are critical when considering cyberspace operations writ large.

Operational Contract Support is the process of obtaining supplies, services, and construction efforts from civilian sources to support military operations (HQDA, 2021, p. 1-1). The ability to hire contractors allows USCYBERCOM to bolster its capabilities, which it cannot create through force generation. Contracted support is paramount to accomplishing cyberspace operations missions.

Similarly, the Army utilizes its Military Personnel, Army (MPA) funding to provide the Cyber Assignment Incentive Pay to offset the difference between military and potential civilian pay. This pay differential rewards Soldiers fulfilling key, critical cyber work roles within the Army (ARCYBER, 2024).

Analysis of OGS Through Leadership

Leadership is paramount across the military, and cyberspace operations are no different. A mission commander on the OGS team described how he identified the vulnerabilities in the ISIS media network. As a captain, he was able to use influence techniques centered around his expertise to convince his supervisor that this idea was feasible. The pair then convinced senior military leadership across USCYBERCOM that their plan was viable, ultimately resulting in OGS itself. They demonstrate high emotional intelligence, the ability to influence beyond positional power

and organizational trust, a willingness of senior leaders to trust their subordinates, and their subordinates' willingness to come forward with ideas throughout USCYBERCOM and the OGS team. Their eventual approval reflected the organization's commitment to fostering initiative and trust. This culture was further validated during the mission's execution when an intelligence analyst provided a mission-critical response to an unforeseen threat. This action demonstrated the operational advantages of a command climate that values subordinate input, empowering leaders to remain agile under unpredictable conditions.

Analysis of OGS Through History

While it may seem unusual to consider cyberspace operations in a historical context due to their recent invention, history provides ways to compare the importance of events, thoughts, and actions over time.

During World War I, aircraft were primarily used for reconnaissance and surveillance (Muller, 1996, pp. 152–154). Towards the end, however, weapons were attached to the aircraft, and a new domain of warfare began to take shape. OGS faced a similar evolution. Initially, cyberspace operations were conducted for purely intelligence purposes. Worldwide events, namely a terrorist attack in Paris in 2015, led to the extension of operations against ISIS. A small "test" operation precluded OGS.

This "precursor" concept was present in World War II. Operation Torch allowed U.S. forces to demonstrate their mettle in combat operations to the Allies. A successful Operation Torch was the precursor to Operation Overlord, just as initial cyber effects operations were the predecessor to OGS.

Historical military thought is also present in cyberspace operations. Carl Von Clausewitz's "fog of war," or the uncertainty present in all military operations, was present during the initial planning for OGS (Clausewitz, 2006). The fog of war allowed the ISIS media network to masquerade itself as a complex system, decreasing the planning team's ability to understand its structure. The fog of war seems omnipresent across all types of military operations.

Implications for Future Joint and Multinational Operations

Analyzing OGS through these lenses provides an opportunity to examine the future.

From the dawn of the internet to the execution of OGS in 2016, the operation represents a culmination of all technological and political acceptance of cyberspace operations and its place in modern warfare. From the Moonlight Maze to Stuxnet to OGS operations, we see a change in political acceptance from total secrecy to modest public discourse surrounding cyberspace operations.

OGS was inherently joint and multinational but was still a very strategic capability. As the U.S. builds partners and allies around the globe, it may become prudent to create a subset of cyberspace operations at the tactical level that can be shared with our multinational partners.

Utilizing the JCIDS process through DOTMLPF, potential solutions arise through the DOTMLPF framework. An organizational solution could be to create a cyberspace operations unit that is organic to the Corps. These organizations could use open-source and non-classified tools, tactics, techniques, and procedures at the operational and tactical levels. These Corps-level assets could then operate in step with Cyber Mission Force (CMF) capabilities to extend these capabilities' reach, scope, and availability.

For example, a Cyber Protection Team (CPT) could deploy to a partner nation in the Indo-Pacific to assess and analyze critical port infrastructure. After their operation, the Corps could deploy its organic cyber unit during routine security cooperation exercises to provide follow-up assessments, analysis, and partner training that builds on the CPT's original work. This redundancy would increase the number of touchpoints with our partner force while supporting potential U.S. interests in port operations in the Indo-Pacific.

In short, the CMF would maintain its strategic capability set while cyber units across the force could leverage non-classified tools to extend the capabilities and incorporate more multinational partners.

Cyber, DIME, and MDO

Cyberspace operations are deeply intertwined with the instruments of national power: diplomacy, information, military, and economic (DIME) powers.

Cyber can be used to gain a diplomatic advantage during international negotiations, exemplified by the espionage of Angela Merkel's cell phone (BBC, 2013). Russia was profoundly influential in the information sphere during the 2016 U.S. elections (FBI, 2018). OGS represents a military application of cyberspace operations. Finally, the Chinese theft of American intellectual property represents an economic facet of cyber operations (House Foreign Affairs Committee, 2020). Cyber operations offer an example of how to analyze the instruments of national power through a single subject. Then, the ability to intertwine many subjects across this model can help leaders understand the complicated and complex nature of our instruments of national power. By mastering this synthesis, leaders are better equipped to design strategies that address the dynamics of modern challenges.

Within the Army, multidomain operations (MDO) are the Army's contribution to the Joint Force. Cyberspace operations are exceptional at providing the MDO tenants depth and convergence when operating on the competition continuum through its ability to apply global effects while supporting operations from the cyberspace domain.

Cyberspace operations are also helpful when creating and exploiting information advantages in support of decision dominance and imposing multiple dilemmas on the enemy, two imperatives of MDO. The Army has traditionally been excellent at integrating land, sea, and air across all levels of warfare, while cyberspace and space operations have traditionally lived in the strategic. Through critical and creative thinking and technological adaptation and innovation, there are ways to integrate cyberspace operations into the operational and tactical levels.

Conclusion

The pace of technology is increasing. While OGS represents a culmination of all development to that point in time, it also represents a springboard into the future. Leaders' ability to analyze future possibilities is paramount to ensuring that the United States is at the forefront of technological solutions. This involves adapting these solutions across all levels of warfare while incorporating our multinational partners.

The analysis of Operation Glowing Symphony through these lenses underscores the need for military leaders to think critically and creatively about the evolving nature of warfare in the digital age. We understand the challenges and opportunities ahead by examining the operation's implications for strategy, tactics, force management, sustainment, leadership, and history. As we strive to integrate cyberspace operations into the operational and tactical levels of warfare, we must remain adaptable, innovative, and committed to developing and integrating cyberspace operations and education for leaders across the Army.

[1] For detailed information surrounding the events of OGS, the author recommends a podcast episode (https://darknetdiaries.com/episode/50/) and an article (https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis).

References

Army Cyber Command (2024). *Cyber Assignment Incentive Pay*. https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/3737184/cyber-assignment-incentive-pay/

BBC. (2013, October 27). US bugged Merkel's phone from 2022 until 2013, report claims. *BBC News*. https://www.bbc.com/news/world-europe-24690055

Clausewitz, C. (1832). *On War*. (2021). Project Gutenberg. https://www.gutenberg.org/files/1946/1946-h/1946-h.htm#chap07

FBI. (2018, July 13). Russian Interference on 2016 U.S. Elections. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections

Forno, R. (2024, December 6). What is Salt Typhoon? A security expert explains the Chinese hackers and their attack on US telecommunications networks. *UMBC*. https://umbc.edu/stories/what-is-salt-typhoon-a-security-expert-explains-the-chinese-hackers-and-their-attack-on-us-telecommunications-networks/

Headquarters, Department of the Army (2021). *ATP 4-10 Multi-Service Tactics, Techniques, and Procedures for Operational Contract Support*, 1-1. HQDA.

Headquarters, Department of the Army (2022). *FM 3-0 Operations*, 3-20. HQDA.

Headquarters, Department of the Army (2023). *FM 3-90 Tactics*, 8-24. HQDA.

House Foreign Affairs Committee. (2020, February). Egregious Cases of Chinese Theft of American Intellectual Property. https://foreignaffairs.house.gov/wp-content/uploads/2020/02/Egregious-Cases-of-Chinese-Theft-of-American-Intellectual-Property.pdf

McConnel, R. A., Mong, J.A., & Ptaschek, D. (2021). Seeing Through the Fog Developing Fog of War Resistant Visualization. *The Military Review*. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/McConnell-Fog-of-War/

Melody, P. (2021). How the Army Runs A Senior Leader Reference Book. *U.S. Army War College*, 2-14. https://usawc-ssi-media.s3.us-east-1.amazonaws.com/pubs/2021-2022_HTAR.pdf

Muller, R. (1996). Close Air Support: The British, American, and German experiences, 1918-1941. In W. Murray & A.R. Millet (Eds.), *Military Innovation in the Interwar Period* (pp. 152–154). Cambridge University Press.

U.S. Joint Chiefs of Staff (2023). *Joint Publication 1, Volume 1, Joint Warfighting*, III-2. JCS.

U.S. Joint Chiefs of Staff (2024). *Joint Publication 5-0, Joint Planning*, IV-22 to IV-27. JCS.

How the Sport of Amateur Radio Direction Finding can Enhance US Army Holistic Health and Fitness and Electronic Warfare Training Objectives

By Lt. Col. Matthew G. Sherburne, P.E.

ARDF participant sprinting towards thier next point. (Photo by Charles Scharlau, USA ARDF Co-Coordinator)

We are always seeking new and innovative ways to enhance the physical and cognitive training of our troops. When we find ways to combine the two, we can enhance the readiness our troops under the heavy demands of combat. One such training activity that supports the Army's Holistic Health and Fitness (H2F) and electromagnetic warfare (EW) objectives is amateur radio direction finding (ARDF), also known as foxhunting, which is based on radio direction finding, orienteering and amateur radio. This national and international sport, also known as radio orienteering, has been around for many decades and combines the even older sport of orienteering with direction finding, which involves locating a radio transmitter. It requires both cardiovascular fitness and mental skill to traverse a course in the woods and urban environments at speed by locating four to five different transmitters. This training focuses on land navigation with a map and compass, the science of antenna and frequency propagation, and radio frequency (RF) direction finding. ARDF is a civilian sport that does not use military RF frequencies or equipment; it is an excellent training activity that any unit can establish either on or off base and has several national level events for U.S. Army personnel to compete. ARDF is an activity that will train our EW force to operate at peak physical and cognitive condition to meet the demands of near-peer adversaries.

During post-World War II, countries, particularly in Europe decided to enhance their military and civilian population expertise in radio direction finding while also honing their land navigation skills through the sport of orienteering. The sport of ARDF began in the 1950s and provided an important civil defense application during the Cold War.[1] It demanded athletes run at neck breaking speeds through the woods to hunt down their beacons by taking multiple lines of bearing. Participants must demonstrate high cognitive ability while operating at peak fatigue to make it through the course. This is precisely the type of activity we need today. In a recent article from *Army Times*, it was reported that, "Army Vice Chief of Staff James Mingus told Soldiers at the Maneuver Warfighter Conference at Fort Moore, Georgia, … that the Holistic Health and Fitness program … will roll out across the entire force."[2] As H2F expands beyond just brigade combat teams (BCTs) and to all units, training activities are needed that units can easily employ. ARDF only requires inexpensive equipment, lots of training land, and an amateur radio licensed control operator.

Amateur radio is leveraged as the licensed means to operate the ARDF radio beacons. In the U.S. and its territories, the Federal Communications Commission (FCC) oversees amateur radio activity under Part 97 of Code of Federal Regulations Title 47 (Telecommunications).[3] Specifically, there are five key purposes of the amateur radio service:

1. To recognize and enhance the value of the

amateur service to the public as a voluntary, non-commercial communication service, particularly in providing emergency communications.

2. To continue and extend the amateur's proven ability to contribute to the advancement of the radio art.

3. To encourage and improve the amateur service through rules which provide for advancing skills in both the communication and technical phases of the art.

4. To expand the existing reservoir within the amateur radio service of trained operators, technicians, and electronics experts.

5. To continue and extend the amateur's unique ability to enhance international goodwill.

Amateur radio governance and operation also exist in many other countries where U.S. forces are located, allowing personnel to engage ARDF around the world. The control operator of the radio beacons must be licensed at the level that authorizes transmission on the amateur radio frequency in use. In the U.S., the FCC has three levels of licensure:

1. Technician Class: This license grants access to limited high-frequency (HF) spectrum but primarily allows operation on very high frequency (VHF) and above.

2. General Class: This license includes all the privileges of the Technician Class, as well as additional access to HF spectrum.

3. Amateur Extra Class: This license provides access to the entire amateur radio spectrum, across all bands.

There are two main bands on which ARDF is conducted: the 2-meter (144MHz) band and the 80-meter (3.5MHz) band. Amateur radio license preparation courses and exams are conducted near or even on many military installations.

Bringing ARDF to your location is an easy process. Setting up ARDF as either a physical training activity or full-scale competition requires finding training land or cantonment areas in which event support personnel will place orienteering flags and amateur radio beacons. It also requires that these areas are mapped to 1:10000 or 1:15000 to allow for the orienteering level of detail required for the sport. Once an area is mapped under the International Specification for Orienteering Maps 2017-2 (ISOM)[4], event organizers will then select locations to place the RF beacons, or foxes, as the community colloquially calls them. With a member of the unit that has earned their amateur radio license, they can setup ARDF beacons with their callsign that gets transmitted automatically by morse code. Event organizers can also use the callsign of a hosting amateur radio club.

The foxes can be built in-house with economical parts. Handheld direction-finding sets are sometimes hard to find on online marketplaces, but they can be built using readily available parts and make for a fun and academic maker lab experience amongst the EW force. There are two

ARDF participant studying a course map. (Photo by Charles Scharlau, USA ARDF Co-Coordinator)

new open-source projects underway in the maker space: SignalSlinger[5], an 80-meter transmitter, and SignalSnagger[6], an 80-meter direction finding receiver with a rough cost of $100 for parts and materials for each. A typical ARDF course will have four to five foxes, along with reprogramming equipment. A unit can then decide if they want to outfit their entire EW platoon[7] with a receiver each or only run a certain number of troops at a time through the course, depending on available unit training funds. As a cost estimate, a unit is looking at $5,000 to establish a five-beacon course and 30 receivers.

With amateur radio and orienteering clubs near most military installations, personnel can find assistance in getting onboarded and setup with ARDF. For units that prefer not to build their own transmitters and receivers from open-source projects, 2-meter and 80-meter kits can be purchased at around $125 for the receivers and $100 for the transmitters from various companies online. It is important to note that 2-meter beacon courses are more difficult for athletes to establish an accurate line of bearing due to reflections that occur at these frequencies.

This fact feeds into the greater skill required on 2-meter courses. 80-meter courses, on the other hand, are easier for athletes to make accurate lines of bearing and recommended for those new to ARDF.

Engaging in ARDF provides many benefits to the Army. It enhances the radio and direction-finding skills of our electromagnetic warfare forces, it provides another physically and cognitively demanding training activity that supports H2F, and it enhances land navigation skills. Experiential knowledge gained during training is the very competitive edge our forces need to win in battle. ARDF is a tested and proven way to get there.

About the author

Lieutenant Colonel Matthew G. Sherburne, USA, is Military Deputy, Army Capability Manager Electronic Warfare, Cyber-CDID, Fort Eisenhower, Georgia. He is an alumnus of the United States Military Academy Orienteering Team and represented the United States in the World University Orienteering Championships held in Slovakia in 2006. He also served as an assistant coach to the USMA Orienteering Team from 2015-2018.

From the author

For further reading, I recommend "Radio Orienteering: The ARDF Handbook," by Titterington et. al.[8] For current information on ARDF and upcoming competitions, please access the American Radio Relay League website on ARDF at https://www.arrl.org/amateur-radio-direction-finding.

Endnotes

1 “About ARDF,” The Wireless Institute of Australia, 2018, https://www.wia.org.au/members/ardf/about.

2 Todd South, “Army to Expand Holistic Health and Fitness Program to All Soldiers,” Army Times, September 12, 2024, https://www.armytimes.com/news/your-army/2024/09/12/army-to-expand-holistic-health-and-fitness-program-to-all-soldiers

3 “Code of Federal Regulations,” National Archives, 2025, https://www.ecfr.gov/current/title-47/chapter-I/subchapter-D/part-97?toc=1.

4 “ISOM 2017-2,” International Orienteering Federation, 2025, https://omapwiki.orienteering.sport/specifications/isom.

5 “SignalSlinger,” OpenARDF, GitHub, 2025, https://github.com/OpenARDF/SignalSlinger.

6 “SignalSnagger,” OpenARDF, GitHub, 2025, https://github.com/OpenARDF/SignalSnagger.

7 “ATP 3-12.4: Electromagnetic Warfare Platoon,” HQDA, January 2023, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN37162-ATP_3-12.4-000-WEB-1.pdf.

8 Titterington, Bob G3ORY, Williams, David M3WDD and Deane, David G3ZOI, “Radio Orienteering, The ARDF Handbook”, Radio Society of Great Britain, 2007..

An Adjustable Budget-Based Detection Toolbox for Contested Spectrum Environments

By 1st Lt Nolan Pearce and Joe Rottner

Electromagnetic Spectrum (EMS) operations in contested environments require battlefield assumptions based on mission dependent factors and complex electronic warfare (EW) concepts. To Soldiers unfamiliar with antenna theory and radio propagation, it can be difficult to visualize the impact of Electromagnetic signatures and the tactical benefit of Electronic Protection (EP) or Electronic Support (ES) operations.

The cyberspace domain, especially the EMS, is a complicated gray space with friendly, adversary, and non-state actors competing for limited spectrum resources. Variables in equipment, terrain, and mission requirements endlessly complicate the following two simple questions:

1. Will friendly forces successfully receive my communications?
2. Will enemy forces be able to intercept my communications?

An input-based toolbox, leveraging foundational wireless communication principles and calculations, allows for instant approximation to the above questions. By abstracting propagation calculations behind a mission-relevant toolbox, Soldiers can stay mission-focused with relevant information about the EMS environment. Current systems regarding EMS operations require operation by a skilled technician and produce more output than decipherable or necessary for a ground Soldier.

Our toolbox, available at https://www.github.com/jrottner/detection_toolbox, uses a series of user inputs and python functions to create EW-based mapping tools. Users can select their waveform, frequency, transmitter power, and link distance under a given detection probability. After calculations are performed, the users are met with a simple “GO/NO-GO” on the success of their communication and the probability of detection from enemy EW equipment along a two-dimensional (2D) map.

The toolbox is endlessly customizable for the addition of new features. While the initial design gives a definitive answer to the probability of success, more waveforms and environmental details may be added for specialized cases. This toolbox will allow its users to gain an understanding of the EMS through experimentation in training and allow for quick solutions in live scenarios.

Background

This toolbox is essentially an endless customizable link budget. Just like a financial budget, factors in the user’s communication link debit or credit the signal strength. If the user finds that their link is unsuccessful between friendly locations, more than just the transmitter power may be changed to achieve mission success.

Link budgets are generally dependent on the following factors:

1. Transmitter power
2. Antennas at both the transmitter and receiver locations
3. Relative locations of the transmitter and receiver
4. Transmission frequency
5. Transmission mode
6. Random or intentional impediments in the environment (vegetation, jamming, etc.)

Design of the toolbox required some design liberty with user input, toolbox-designated specifications, and output. For example, while the user will often change parameters such as frequency, link distance, power, and modulation scheme, it is assumed that the ability of an enemy detector will remain constant. Similarly, it is assumed that a successful communication link – meaning, the transmitted signal received above a certain signal-to-noise ratio (SNR) – will stay the same for each mode regardless of implementation.

For this initial toolbox, frequencies were customizable within the very-high/ultra-high frequency (VHF/UHF) range. This range is the most closely comparable for point-to-point communication links and involves the simplest forms of wireless channel effects. In HF links below the VHF range (less than 30 MHz), wireless signals potentially bounce multiple times between the earth's surface and the ionosphere. Links in the UHF range (300MHz-3 GHz) are often used for satellite links with greater range and greater antenna array performance at a similar physical size. The penalty paid for these higher frequencies is more atmospheric absorption or other phenomena. These links may require weather-dependent factors unnecessary for a simple line-of-sight (LOS) link. Therefore, the toolbox will focus on the more operationally relevant VHF/UHF frequency bands for LOS operation predictions.

Currently, many industry standards exist for wireless propagation modeling over certain terrain. As more cellular networks come online, telecommunication companies often need to identify possible weaknesses in cell tower locations or in indoor wireless environments. The Free-Space Path Loss model primarily uses the distance between transmitter and receiver to identify the power lost over this link but relies on free space assumption that there is no terrain, vegetation, or buildings between the two points. However, the Hata model accounts for these scenarios and the Hata adjusted model allows for customization in rural and suburban environments. The Hata and Hata adjusted model appear to track real-world path loss more closely than the simplistic Free Space Path Loss model. We proceed with these more descriptive models to balance more predictive performance while simplifying the amount of descriptive input information needed by the operator.

To define success in the toolbox environment, a user must achieve a higher received SNR than the minimum viable SNR at the receiver's location. This means a signal will be received with more than enough power to be successfully decoded. The received SNR is calculated using a link budget approach with options to select various modeling algorithms for the distance-based path loss from the transmitter to the receiver. The minimum SNR, however, is calculated as an assumption based on the Shannon-Hartley Theorem. This theorem states that a communication environment has a maximum capacity for transmission (in bits / second) for a given SNR and signal bandwidth; by using a given data rate and bandwidth for common military signals, the minimum viable SNR can be found.

Users cannot change the minimum viable SNR. However, the SNR determined by the link budget calculation will be updated if the user changes their test parameters – for example, the user can move their radio locations closer together and will see a higher SNR because of the decreased distance.

Calculation of enemy interception underwent a similar application. To find the maximum intercept distance, the minimum viable SNR was used as the receiver signal strength. From here, the maximum distance possible while still achieving a successful link could be found from the transmitter. This gives a likely area where other forces could intercept the transmission given the experimental variables.

These calculations only identify data points – the received SNRs – possible at given locations. However, geographic mapping tools allow for easily interpretable results. The SNRs are first converted to "GO" values if they are greater than the minimum viable SNR and "NO-GO" otherwise. These values, assigned to their relevant coordinate grid location, appear as a "heatmap" on a map of the link location. Overall, these outputs easily allow users to identify the strength of their communication link and see possible enemy intercept areas.

Application

A simple application for this toolbox is a point-to-point single-channel ground and airborne radio system (SINCGARS) VHF link between two whip antenna stations. In the toolbox, two arbitrarily selected points were used to test this link. The transmitter was placed at Barton Field in Fort Eisenhower, GA, and the receiver at the first tee of the Masters Course in Augusta, establishing a reasonable 13km link distance for VHF Line-of-Sight. The user selects omnidirectional antennas

for both radios and uses the Free-Space Path Loss model due to the relatively unrestricted and flat terrain between the two points.

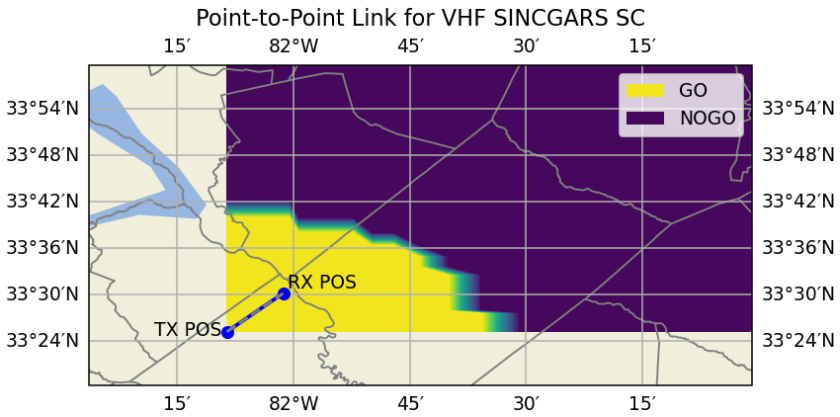


Figure 1: Toolbox output depicting a 25W SINCGARS Radio at 80 MHz in Fort Eisenhower, GA

After running the calculation, the user is presented with a "GO/NO-GO" on successful link establishment and a heatmap of the received SNR. Using the calculations previously mentioned, VHF SINCGARS requires around 4 dB minimum viable SNR. Based on the link, the path loss between the two points is around 9dB. Therefore, the user needs a transmission power of at least 13 dB or 20 watts.

Similarly, the user can see an approximate range of detection from their transmitter point. If the simulation started with 25W of transmitter power, the detection range extends a few kilometers outside of the receiver's range. This

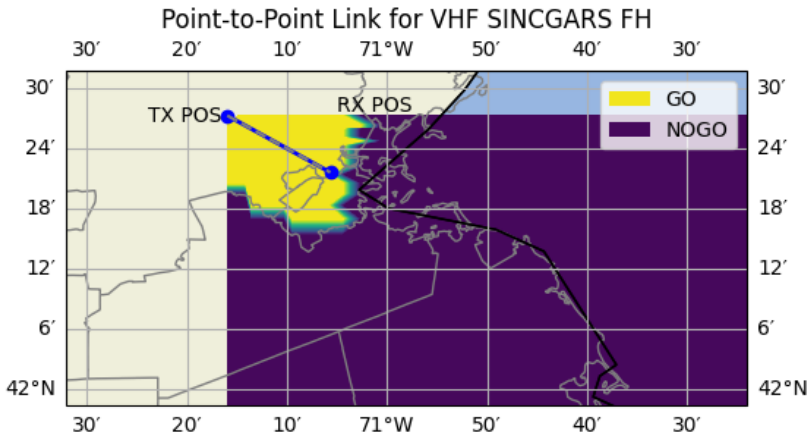


Figure 2: Toolbox output depicting a 20W SINCGARS FH Radio at 120 MHz in Lexington, MA.

may encourage the user to limit the transmitter's power for a lower probability of enemy detection or interception.

Users can test SINCGARS frequency hop (FH) with a directional Yagi-style antenna at the transmitter. Locations for these transmitters were set at MIT Lincoln Lab's Katahdin Hill and the MIT Library in Cambridge, MA. The main lobe of the Yagi antenna clearly allows for more selective communication towards the friendly receiver station. Similarly, the FH mode increases the effective range of the radio by allowing a lower minimum viable SNR at the receiver. Starting from the same 20W transmitter power, the minimum viable SNR is 4 dB along the axis of the main lobe of the directional antenna. Because the transmitter station is in an elevated position (roughly 100 meters), its effective range is similarly increased. Enemy detectors will generally need to stay in the main lobe of the antenna to successfully intercept friendly communications.

Given the option to tweak simulation parameters, Soldiers should be able to identify potential advantages and vulnerabilities in their EW arsenal. Even for a simple point-to-point radio check, the toolbox will allow for a broader understanding of EMS signatures and operations within congested environments.

Additional Research

The electromagnetic spectrum is a constant-changing battlefield. However, its backbone of theorems, algorithms, and assumptions remain constant. Open-source mapping functions and calculations, derived from common military EW assets, enabled the creation of a toolbox useful for testing link fidelity.

This toolbox can expand in several different research areas. First, more communication modes, frequency ranges, and radio profiles can always be added to suit each individual battlefield need. Modern communication modes often employ anti-jam and anti-detection methods that would enable successful communication much further than calculated using simple single-channel SINCGARS. For example, packet and digital FM amateur radio modes both occupy

the same frequency range as FM voice, but can travel further distances due to their lower bandwidth. Automatic link establishment (ALE) would allow for communications over greater distances using the HF frequency range. Improvements in path loss modeling for frequency hop systems – namely, doppler fading and wideband scattering – would give a better picture to the EMS impacts towards transmitted signals. Likewise, recent advancements like the Trellis TSM® waveform and mobile ad-hoc network (MANET) systems require further analysis to determine a minimum viable SNR for the toolbox.

The toolbox currently calculates its received signal criteria based on input conditions. However, the inverse could also be calculated – the toolbox could suggest what optimal frequency modes, locations, and antennas should be implemented for a given set of environmental conditions.

Statistical modeling could improve the decision-making output from the simulation. Calculations with the probability density function will produce the outage probability, or the percent chance that a signal will fall below the minimum viable SNR. Instead of the produced "GO/NO-GO", the simulation could give a probability heatmap of expected outages.

The toolbox can also be implemented in any number of training environments due to its low complexity and simple python framework. Link budget calculations could be added to the Team Awareness Kit (TAK) suite for greater situational awareness in a congested spectrum environment.

Conclusion

The cyberspace domain is mired in uncertainty. Environmental and mission variables complicate whether or not a link exists between friendly radios. This toolbox would help to clearly and reliably inform Soldiers of the feasibility and possible risks of EMS operations, while enabling a greater tactical understanding of communication principles as it relates to the mission.

Author Bios

1st Lt. Nolan Pearce is a 17A Cyber Basic Officer Leadership Course (BOLC) Student in Fort Eisenhower, GA. He has a B.S. in Electrical Engineering from the United States Military Academy and a M.S. in Electrical and Computer Engineering from Northeastern University. Pearce's research interests lay in radio propagation, next-gen 5G, array processing, and beamforming. His previous work experience includes postgraduate research as a military liaison at Massachusetts Institute of Technology's Lincoln Laboratory. He holds an extra-class amateur radio license.

Joe Rottner is an Associate Staff at MIT Lincoln Laboratory in the Tactical Edge Communications Group. He holds a B.S.E. and M.S.E. from the University of Michigan in Electrical Engineering with a focus in Wireless Communications. Joe's research interests mainly fall into waveform/communications standards design, wireless analysis, and optimal detection/estimation techniques.

Acknowledgements

The code for the toolbox can be found at https://www.github.com/jrottner/detection_toolbox/ under an MIT Open Use license. All information for wireless propagation was taken from Andrea Goldsmith's 2020 Wireless Communications textbook, freely available through the Stanford University website. We encourage any collaboration or suggestions for this toolbox.

The Strategic Importance of Timing in Assured Positioning, Navigation, and Timing (APNT) for the U.S. Army

By Dave May, Senior Cyber Intelligence Advisor

AI generated illustration

Abstract

Timing plays a foundational role in Assured Positioning, Navigation, and Timing (APNT), which is essential for modern military operations. The U.S. Army depends on precise timing to synchronize its communication networks, navigation systems, and precision weaponry. In contested environments, adversaries use electromagnetic and cyber warfare to disrupt these capabilities, emphasizing the need for robust, resilient timing systems. This article examines the strategic role of timing in APNT, highlights the challenges to maintaining reliable timing, and explores the Army's ability to exploit adversarial timing systems through cyberspace and electromagnetic warfare, providing a decisive edge on the battlefield.

Introduction

In the complex and dynamic landscape of modern warfare, timing is the underlying foundation that enables nearly every operational aspect of the U.S. Army. From coordinating large-scale maneuvers and delivering precision-guided munitions to ensuring secure communication, timing serves as the invisible thread that weaves disparate systems and units into a cohesive force. The importance of timing is particularly evident in the Global Positioning System (GPS), which relies on extremely precise timing to determine positioning. For decades, operational forces have depended on GPS for accurate timing, and the Army's ability to operate effectively has become increasingly reliant on this capability. To address the growing threat of disruption, the Army has developed Assured Positioning, Navigation, and Timing capabilities, which ensure the continuity of operations even in the face of advanced adversary tactics.

As the threat landscape continues to evolve, the criticality of timing in APNT has become even more pronounced. In environments where ad-

versaries employ sophisticated electromagnetic and cyber warfare techniques, the vulnerability of systems that rely on precise synchronization is exposed. Threats such as GPS jamming and spoofing attacks can significantly degrade operational capabilities, highlighting the need for innovative solutions to protect Army systems and exploit those of its adversaries. This article will explore the strategic importance of timing in APNT, examine the challenges posed by modern threats, and discuss the cutting-edge measures being implemented by the U.S. Army to maintain its operational edge.

The Role of Timing in Modern Military Operations

The importance of timing is evident across multiple domains. Accurate timing allows military units to securely coordinate across vast geographical areas, ensuring seamless execution of complex missions. Without precise timing, communication networks or their security would falter, leading to delays, failures, or compromises in the transmission of critical information. Similarly, GPS-dependent navigation systems rely on nanosecond-level timing accuracy to deliver precise positioning data. A single timing error can result in significant positional inaccuracies, potentially jeopardizing mission outcomes.

In addition to its role in communications and navigation, timing is crucial for weapon system effectiveness. Precision-guided munitions, for example, depend on synchronized timing to calculate trajectories and deliver payloads accurately. Disruptions in timing can compromise these systems, resulting in missed targets or unintended collateral damage. The Army's reliance on timing extends to logistical operations, where synchronized efforts ensure the efficient movement of troops, supplies, and equipment.

Challenges to Timing in Contested Environments

In today's contested environments, maintaining reliable timing is increasingly challenging. Adversaries employ electromagnetic warfare tactics, such as GPS jamming and spoofing, to disrupt U.S. systems. These tactics can deny the availability or degrade the accuracy of positioning and navigation systems, forcing units to operate with reduced capability. Natural disruptions, such as space, weather, or obstructions caused by urban or dense environments, further complicate the reliability of timing systems.

The Army also faces vulnerabilities within its own infrastructure. Systems that rely heavily on satellite-based timing are susceptible to cyberattacks and electromagnetic interference. As adversaries develop more advanced techniques, the risk of timing disruptions grows, emphasizing the need for resilient and redundant solutions.

Exploiting Adversarial Timing Systems

While ensuring the resilience of its own timing systems, the U.S. Army actively seeks to exploit vulnerabilities in adversarial timing capabilities. Through advanced cyberspace and electromagnetic warfare operations, the Army can manipulate, degrade, or disrupt enemy timing systems, creating significant operational advantages.

Cyber operations allow for the infiltration of adversarial systems to corrupt their timing mechanisms. By introducing errors or delaying synchronization, the Army can disrupt the enemy's ability to coordinate effectively. Electromagnetic warfare techniques, such as precision jamming, can degrade PNT signals used by adversaries, forcing them to rely on less accurate means. Advanced spoofing methods can also be employed to send false timing signals, misleading adversaries and creating opportunities for exploitation.

By targeting adversarial timing provisioning systems and their clients, the Army not only disrupts enemy operations but also creates confusion and delays, reducing their ability to respond effectively. These techniques are particularly effective in undermining trust in available information and the coordination of large-scale operations, logistics, and command structures.

Resilient Timing Solutions

To address the challenges of timing disruptions, the U.S. Army is investing in advanced technologies and alternative systems that ensure operational resilience. One approach involves enhancing access to GPS timing using anti-jam antenna systems and other techniques. Additionally, the Army is improving the integration of available systems, including inertial measurement units (IMUs) and networked timing sources, while

also incorporating backup timing solutions such as atomic clocks. This multi-layered approach enables precise timing and navigation even in the absence of GPS signals. Furthermore, the development of non-GPS alternative positioning, navigation, and timing (PNT) sources, such as terrestrial and celestial methods, provides additional layers of redundancy for client systems, enhancing overall system resilience.

The integration of emerging technologies, including artificial intelligence (AI) and machine learning, is also being leveraged to enhance the predictive capabilities of APNT systems. By harnessing these tools, the Army can anticipate potential disruptions, implement proactive countermeasures, and gather critical information about adversary activities. This proactive approach enables the Army to stay ahead of emerging threats and maintain a strategic advantage in the face of increasingly sophisticated timing disruptions.

Operational Implications of Timing

The synchronization enabled by accurate timing has far-reaching implications for military operations. It ensures that units can maneuver effectively, communicate securely, and deliver precision strikes with minimal collateral damage. Timing also supports strategic decision-making by providing commanders with accurate and timely situational awareness.

Additionally, the integration of cyberspace and electromagnetic warfare into timing operations underscores the importance of dominating the information and electromagnetic domains. By protecting its own systems and exploiting adversarial vulnerabilities, the U.S. Army maintains a critical edge in both tactical and strategic operations.

Conclusion

Timing is the foundation of Assured Positioning, Navigation, and Timing and is essential for the U.S. Army's success in modern warfare. As adversaries continue to develop advanced disruption tactics, the Army must prioritize the development and integration of resilient timing solutions. At the same time, leveraging cyberspace and electromagnetic warfare to exploit adversarial timing systems provides a decisive advantage, enabling the Army to maintain its superiority on the battlefield. By addressing these challenges and seizing opportunities, the Army ensures its readiness to operate effectively in the complex and contested environments of the future.

Gray Space

Cyber & Electromagnetic Warfare Journal

Want to be featured on the next cover?

Photographs should be at least 1MB or higher and highlight Cyber or Electronic Warfare. Soldier images are also allowed. Full name, rank, and unit of Soldier(s) in the photo must be included with a short description explaining the photograph. AI generated photographs are also accepted.

Send to:

vincent.j.kirk3.mil@army.mil or

usarmy.eisenhower.cyber-coe.mbx.the-gray-space@army.mil

Fall 2025 Themes:

- Military Operations
- Strategy and Tactics
- Stewardship of the Profession
- Innovation
- Education and Training
- Cyber and EW Convergence

PIN: 220975-000