780th MILITARY INTELLIGENCE BRIGADE (CYBER)

THE BYTE

Vol. 14, Issue 2

April 2026

ARTIFICIAL INTELLIGENCE:
At the Unit of Action

780th MI BDE
"STRENGTH AND HONOR"

COL Candy Boparai
Commander
CSM Joseph Daniel
Command Sergeant Major

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

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

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

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

On the Cover

Brigade Best Squad Competition

FORT A.P. HILL, Va. – Army Sgt. Ángel Jesús Martínez serves in the 781st Military Intelligence (MI) Battalion (Cyber), Vanguard, Fort George G. Meade, Maryland, and he was in a squad which competed and won the 780th MI Brigade (Cyber) Best Squad Competition held March 3 to 5, 2026. Martínez's squad will represent the brigade at the U.S. Army Intelligence and Security Command BSC, April 15 to 21, 2026.

FROM THE COMMANDER:

The battlefield has always rewarded those who see first, decide fastest, and act with precision. Today, that edge increasingly belongs to those who understand artificial intelligence — not as a distant technology, but as a present and potent instrument of national power.

This edition of The BYTE arrives at a pivotal moment. Across the government and defense enterprise, Artificial Intelligence (AI) is no longer a research curiosity or a budget line item buried in a future-year program. It is being deployed now — in threat detection, network defense, adversarial analysis, and even offensive cyber. The questions are no longer whether AI belongs in this space, but how we wield it responsibly, effectively, and with strategic intent.

The articles that follow explore this terrain from multiple angles. Our contributors examine how machine learning is reshaping the way analysts sort signal from noise, how autonomous systems are accelerating the tempo and scale of cyber operations, and where human judgment must remain firmly in the loop. We also wrestle honestly with the harder questions: adversarial AI, legal and ethical boundaries, and the risks of over-reliance on systems we do not fully understand.

What unites these perspectives is a shared conviction that technological advantage is earned, not given. Integrating AI into government cyber operations requires more than acquiring capable tools — it demands informed professionals who can interrogate outputs, recognize limitations, and make sound decisions under pressure.

We hope this edition sharpens your thinking and sparks the kinds of conversations our mission depends on.

Candy Boparai
COL, CY
Commander, 780th MI BDE (Cyber)
"Everywhere and Always…In the Fight!"

PRAETORIANS

The Dawn of a New Era: Embracing AI as Our Next Force Multiplier

By Mr. Aaron Tipton, Senior Civilian Advisor, 780th Military Intelligence Brigade (Cyber)

THIS WITH GREAT PLEASURE THAT I INTRODUCE THIS PUBLICATION'S THEME: "*Artificial Intelligence at the Unit Of Action*." The collection of articles you are about to read represents a snapshot of a pivotal moment in our organization's history. We are at the cusp of a technological revolution, one that promises to reshape our work, enhance our capabilities, and ultimately, make us more effective in our mission to protect the nation. The question is no longer if we should adopt AI, but how we can do so thoughtfully, strategically, and with a clear-eyed view of both its potential and its challenges.

We cannot afford to be laggards in the age of artificial intelligence. The good news is, as you will read in these pages, our workforce is already leaning forward, exploring and experimenting with these new tools. From the 781st's innovative use of AI in their CTE range, as detailed by 1st Lt. Tadeusz Sikorski, to the 782d's practical applications in cyber intelligence and daily duties, our people are proving that coffee is, indeed, no longer the only productivity tool.

Making Our Work Lives Easier: AI in Administrative Tasks

One of the most immediate and tangible benefits of AI lies in its ability to streamline the administrative tasks that, while necessary, can often feel like a drag on our time and creativity. As Capt. Laura Wissmann and 2nd Lt. Nicolas Jimenez articulate in their pieces, AI is a powerful force multiplier, not a replacement for human ingenuity. This is especially true when it comes to the administrative burdens that we all face.

Consider the simple act of writing an email or a report. We've all been there, agonizing over phrasing, grammar, and tone. Now, imagine having an AI assistant that can proofread your documents for clarity, suggest more concise language, and even help you tailor your message to a specific audience. This is no longer science fiction; it's a capability that is available to us right now.

Or take, for example, the often-dreaded task of establishing civilian performance objectives in DCIPS. Crafting meaningful, measurable, and impactful objectives is an art form. AI can be an invaluable partner in this process. By providing the AI with your job description, your team's goals, and the overarching strategic objectives of the organization, you can generate well-written, relevant performance objectives in a fraction of the time it would normally take. This allows you to focus on the more human-centric aspects of performance management, such as mentoring, coaching, and providing constructive feedback.

A Balanced Perspective: Navigating the New Landscape

Of course, with any new technology, there are challenges and pitfalls to be aware of. 1st Lt. Alexander Enriquez's article, "AI and I: How Cyber Soldiers are Using Artificial Intelligence in their Daily Duties," provides a candid look at the "good and bad use cases" of AI. He wisely cautions us about the phenomenon of "hallucination" answers, where the AI can produce responses that sound plausible but are factually incorrect. This is why, as Maj. Austyn Krutsinger points out in his fascinating piece on using AI in binary analysis, a human must always remain in the loop to review and validate the AI's output.

The Way Forward: A Call to Action

The articles in this publication, from 1st Lt. Kamy Shah's exploration of AI as a force multiplier in cyber intelligence to the broader discussion on the future of code development in "The End of the World as We Know It: AI shaping how we produce code," all point to a common theme: the future is a partnership between humans and machines. Our role is not to be passive consumers of this technology, but active participants in its development and deployment.

I encourage each and every one of you to read these articles, to reflect on their implications for your own work, and to start a conversation with your colleagues and leadership about how we can best leverage AI to our advantage. The journey ahead will be one of continuous learning and adaptation, but I am confident that by working together, we can unlock the full potential of artificial intelligence and, in doing so, build a more efficient, effective, and innovative organization for the future.


US ARMY

AI and the Cyber CTE

By 1LT Tadeusz Sikorski, 781st Military Intelligence Battalion (Cyber)

AS PART OF FULFILLING CYBER NATIONAL MISSION FORCE PRIORITIES, the Cyber Training Environment's earliest requirements included the need for a dedicated AI target. Whatever your personal feelings on the state of AI, it is undeniable that organizations around the world are adopting these systems and exposing them to the open internet and internal networks. AIbased attacks therefore present an opportunity for targeting and access generation, and it is vital that we familiarize and train our operational elements on future technologies.

There are multiple challenges with implementing AI in a range environment. The first is resourcing, with powerful AI models requiring equivalently powerful hardware, but there is significant complexity in implementing such hardware on the PCTE range network. Servers and GPUs plugged into a TS (top secret) network must remain on a TS network even after exercise execution, and the rapid progress of AI models can easily leave a range falling behind. Deliberate planning in terms of hardware procurement and utilization needs to be made. To some extent, this leaves very expensive GPUs as expendable items. The CTE ended up running a CPUoptimized model, since CPU cores are essentially unlimited on PCTE.

The second challenge is model selection, with the need for local model execution and rapid responses to operator input leading to a focus on small, compact opensource models. These models often lose context and do not competently retain their system prompts, which led to a long development and tuning process.

Ultimately, these flaws were overcome by the AI lead for PCTE, Army 1st Lt. Chandler Hake, who narrowly focused the model on two agentic tools and enforced a simple set of checks on tool execution. In this case, to trigger any effect, the operator would have to use the word "please." This simple check was designed to teach operators the basic concepts of prompt injection. The model and scenario presented were not complex enough to stand up to serious scrutiny in the long term, and so the operator attack duration was limited to a single day's worth of prompting.

For future iterations and any AIrelated training, it is, in my view, very important to focus on small, discrete modules and capabilities. Instead of trying to create a grand model covering all AI aspects, a tightly focused model with discrete hardware requirements aimed at training a specific TTP (tactics, techniques, and procedures) is likely to vastly lower resource and development requirements. Additionally, the Cyber Mission Force should work to procure GPU hardware for use in training and range environments.

** Persistent Cyber Training Environment (PCTE)*

Teaching Old Disassemblers New Tricks: Turning a Large Language Model (LLM) into an Intern Who Actually Reads the Manual

By MAJ Austyn Krutsinger, Detachment Hawaii, 782d Military Intelligence Battalion (Cyber)

WE HAVE ARTIFICIAL INTELLIGENCE (AI) TOOLS available to us and people want to "just use AI" yet sometimes lack understanding of which problems AI is suited to help solve. Binary analysis for reverse engineering represents one specific use case where AI can help save time and increase operational capacity when used correctly. This article outlines how we can use large language models (LLM) to help translate and articulate the language of a disassembler into the language of humans. This LLM-assistance can be great for helping find vulnerabilities – whether analyzing adversary malware, assessing third-party software, or securing your own code. Reverse engineering and binary analysis are a tedious task that requires one to keep a lot of context-specific details in their mind while attempting to understand a language designed for a computer. It's almost like putting a jigsaw puzzle together but not only being allowed to "put" every other piece together and only when you can exactly remember having seen the middle connecting piece. Not a perfect analogy, but the point is there can be a lot of contexts one has to remember.

Reverse engineering software may come with a few terms that are not a part of everyone's vernacular. Reverse engineering is the process of understanding how, in this context, exactly a computer program functions. That is, what the computer is doing to the bits and bytes of data in a computer's memory. Large Language Models are a mathematical construct (multi-dimensional tensors, specifically) that assigns a word to a number and follows a path through this mathematical construct where the next number holds a higher or lower probability based on many of the previous numbers. We can then replace this "path" of numbers with the respective words and see the generated stream of words in the form of a sentence, paragraph, etc. Let me give you an example to help articulate what I mean. If I were to say, "I saw a beautiful bird and it's color was…." You know that words like red, green, yellow, etc. have a much higher probability than words like leadership, spaghetti, or was. Your brain has some kind of probabilistic prediction, and we can mathematically represent this in the form of LLMs. A compiler is a piece of software that can trivially turn high-level language into machine code, but the inverse is not true. A decompiler is a piece of software that attempts to turn a computer's assembly language into a quasi-readable interpretation of the code's high-level representation. (Note: Feel free to research the P vs NP problem to understand why this kind of unidirectional conversion is difficult.) The problem for reverse engineering is the compilation process removes a lot of context-specific meaning. Instead of getting a function name like `important_data_processing_thread()`, you will get something like `sub_10034586()`. I think anyone would agree that one of those function names hold a little more meaning to the reader than the other. Because LLMs, and all other machine learning tools, excel at finding patterns in data, we can use LLMs with pretty good success for interpreting the meaning based on the data the LLM was trained with that may have similar patterns. LLMs can be like an adult's mind in a toddler's body – they seem to understand the world – just still do unexpected and odd things sometimes. A human still needs to take time and review the LLMs analysis, but we can do hours to weeks' worth of work when really needing to dig into the inner working of large, compiled programs.

A "tiny" computer program nowadays can be hundreds of kilobytes in size. This means there can be tens to hundreds of thousands of instructions for the computer to execute. Somewhere buried in those thousands of instructions could lay literally one instruction that doesn't check one byte of memory in which a malicious user can send a custom string of bytes for that program to process, and potential execute code not originally intended for the program to execute. It's not a problem of finding a needle in a haystack, rather a needle in a needlestack. There are techniques to scope down the amount of information to dig through, but the processes can still take a human a considerable amount of time. Computers are good at processing lots of bytes of data at one time, and subsequently, LLMs can process many numbers at a time, say for instance the bytes of a computer program. Because LLMs are trained on data that has patterns of reverse engineered code, and because programs tend to have similar patterns in code for processing data, LLMs can often do a decent job at finding such patterns and finding them faster than humans. Where a person can read thousands of lines of assembly language in days, an LLM can "read" those lines in seconds.

Now, I'm not making a new-age tale of John Henry and the steam powered drill. This is human vs. machine, rather human with machine where we can use the right tool for the job. Finding patterns in data is a great use case for "AI". To be able to effectively use the tools available to us, we must educate ourselves and understand the kinds of problems technologies can solve. Today, we all have a fundamental understanding of how we can use a computer. There are so many pieces of

software we're familiar with and have developed an intuition for which software can solve certain problems. "AI" is a new technology and often mis-understood, so we don't often pair the AI tool with the right kind of problem. I challenge us all to do a better job defining the problems we want to solve. If we replace the word "computer" with the word "AI" and realize a statement like "Let's use computers to accelerate decision making" is too broad and doesn't define the problem well enough to implement a solution, then when we say "Let's use AI to accelerate decision making" is also too broadly scoped.

AI is a great tool and a productivity multiplier when used for the right kind of problem. Reverse engineering software is a problem that's operationally relevant to the 780th MI Brigade's mission. Building a better intuition for the other kinds of problems is how the organization can accelerate effective use of the new technology. ■

AI Empowering the Warfighter, Not Replacing

By CPT Laura Wissmann, Detachment Texas, 782d Military Intelligence Battalion (Cyber)

THE MODERN BATTLEFIELD IS NO LONGER CONFINED TO PHYSICAL DOMAINS; it has expanded into the complex digital landscape where data is as critical as ammunition. In this new era, Artificial Intelligence (AI) is emerging as a transformative force, not just in combat, but in the crucial, yet often overlooked, realm of military administration. By automating and streamlining time-consuming administrative tasks, AI is freeing up Soldiers to focus on their core mission requirements. This change ultimately enhances productivity and operational readiness.

The administrative burden on Soldiers is a long-standing challenge. From personnel management and logistics to intelligence analysis and reporting, these tasks, while essential, can divert valuable time and attention away from mission-critical activities. However, the integration of AI is available to revolutionize these processes, offering a future where Soldiers are augmented by intelligent systems that handle the mundane, repetitive, and data-intensive aspects of their work.

One of the most significant impacts of AI is in the area of data processing and analysis [11, 4]. The sheer volume of information generated in modern military operations is staggering, and manually sifting through data is a monumental task. AI algorithms can rapidly process and analyze vast datasets, identifying patterns, and extracting actionable intelligence that would be impossible for human analysts to detect alone [7]. This capability is not only crucial for battlefield awareness but also for administrative functions such as predictive maintenance for military readiness, which can reduce downtime and ensure that assets and resources are ready when needed [10, 11].

Furthermore, AI is streamlining logistical and personnel management [11, 7]. AI-powered systems can optimize supply chains, predict demand for resources, and manage the deployment and readiness of personnel [10]. This frees up Soldiers from the complexities of paperwork and resource allocation, allowing them to concentrate on training and mission execution. For instance, the U.S. Army has already demonstrated the power of AI by using it to update 300,000 personnel descriptions in a single week, a task that would have taken an individual over five years to complete [12].

The benefits of AI extend to enhancing individual Soldier productivity and decision-making. AI-driven tools can provide real-time information and decision support, reducing cognitive load and enabling faster, more informed choices in high-pressure situations [8, 10]. This can range from providing guidance on managing potential dangers to offering real-time language translation in multinational operations [10, 9]. By offloading these cognitive burdens, AI empowers Soldiers to focus on the strategic and creative aspects of their roles.

While the potential of AI in military administration is immense, it is not without its challenges. The ethical implications of AI, particularly in autonomous systems, require careful consideration and the development of robust governance frameworks [1, 4]. Ensuring the reliability, security, and

transparency of AI systems is paramount to successful and responsible integration into military operations [2, 7]. Moreover, the risk of "automation bias," where human operators over-rely on AI-generated information, must be mitigated through proper training and the maintenance of human oversight [1].

Despite these challenges, the trajectory is clear: AI will play an increasingly vital role in modernizing military administration. By shouldering the administrative load, AI is not replacing Soldiers but empowering them. It is creating a future where Soldiers are more focused, more productive, and better equipped to meet the complex demands of 21st-century warfare. The Cyber Soldier, augmented by AI, will be a more effective and efficient warfighter, ready to face the challenges of a rapidly evolving global security landscape.

Reference:

[1]Batallas, C. (2024, October) When AI Meets the Laws of War. https://www.ie.edu/insights/articles/when-ai-meets-the-laws-of-war/

[2]Bennett, N. (2025, May) 100+ AI Statistics Shaping Business in 202. https://www.venasolutions.com/blog/ai-statistics

[3]Brandon III, C. T. (2025, September 18). OPTIMIZING MILITARY EFFICIENCY. The United States Army. Retrieved February 4, 2026, from https://www.army.mil/article/288138/optimizing_military_efficiency_

[4]Finabel. (2023). Artificial Intelligence and the Future of Warfare. https://finabel.org/wp-content/uploads/2024/07/FFT-AI-and-the-future-of-warfare-ED.pdf

[5]Lacroix, E. B. (2023, August 1). Future of Army Logistics | Exploiting AI, Overcoming Challenges, and Charting the Course Ahead. The United States Army. Retrieved February 4, 2026, from https://www.army.mil/article/267692/future_of_army_logistics_exploiting_ai_overcoming_challenges_and_charting_the_course_ahead

[6]Márquez-Díaz, J. E. (2024). Benefits and Challenges of Military Artificial Intelligence in the Field of Defense. Computación y Sistemas, 28(2). https://doi.org/10.13053/cys-28-2-4684

[7]Malik, H., Afridi, S. (2024, December). The Role of Artificial Intelligence in Modern Warfare and International Security. https://www.researchgate.net/publication/386341455_The_Role_of_Artificial_Intelligence_in_Modern_Warfare_and_International_Security

[8]National Intelligence Council. (2021, March). Deeper Looks: The Future of the Battlefield. Office of the Director of National Intelligence. Retrieved February 4, 2026, from https://www.dni.gov/index.php/gt2040-home/gt2040-deeper-looks/future-of-the-battlefield

[9]NSTXL. (2023, January) Military AI is Changing Defense Strategy. https://nstxl.org/military-ai-is-changing-defense-strategy/

[10]Parangat. (2024, October). How Artificial Intelligence (AI) is Evolving the Future of Military Defense Approaches. https://www.parangat.com/how-artificial-intelligence-ai-is-evolving-the-future-of-military-defense-approaches/

[11]Sentient Digital, Inc. (2023). The Most Useful Military Applications of AI in 2024 and Beyond. Retrieved February 4, 2026, from https://sdi.ai/blog/the-most-useful-military-applications-of-ai/

[12]United States Army Public Affairs. (2025, May 15). Army launches Army Enterprise LLM Workspace, the revolutionary AI platform that wrote this article. The United States Army. Retrieved February 4, 2026, from https://www.army.mil/article/285537/army_launches_army_enterprise_llm_workspace_the_revolutionary_ai_platform_that_wrote_this_article

[13]United States of America. (2025). Resolution 79/239 "Artificial Intelligence in the military domain and its implications for international peace and security". United Nations. Retrieved February 4, 2026, from https://docs-library.unoda.org/General_Assembly_First_Committee_-Eighteth_session_(2025)/79-239-US-EN.pdf.

AI and I: How Cyber Soldiers are Using Artificial Intelligence in their Everyday Work Life

By 1LT Alexander Enriquez, 782d Military Intelligence Battalion (Cyber)

RECENTLY, A FRIEND ASKED ME WHICH WAS LARGER: A MILE OR A NAUTICAL MILE. Neither one of us could remember, but we had a vague idea that a nautical mile was shorter than a mile. We decided to ask an Artificial Intelligence (AI) model what a nautical mile was. It responded that a nautical mile was equal to approximately 1.15 miles. I told my friend that this conversion meant that a mile was a smaller unit of measurement, while my friend held onto his belief that the conversion made a nautical mile smaller than a mile. We once again asked AI. This time, we were more direct and asked it which was smaller: a mile or a nautical mile. It responded: "The nautical mile is smaller than the statute mile (often simply referred to as a 'mile') because they are based on different historical and geographical definitions." I was confused. To me, the math suggested that a nautical mile was larger, but here, the answer was exactly the opposite. Then I noticed that my friend had worded his question a bit oddly. He did not ask "which is larger," as I had thought. He asked the AI "why is a nautical mile smaller?" The AI responded with what it thought he wanted. The facts were available, but the words the AI provided as an answer were incorrect.

I have remained suspicious of AI's usefulness when presented with anecdotes like the one above. I decided to ask around the 782nd Military Intelligence (MI) Battalion to get a sense of how Soldiers were using AI. I found that many Soldiers find AI incredibly useful and are well aware of its limitations.

One way that Soldiers in the 782d are using AI, as one Cyber Planner I interviewed put it, is as a "glorified search engine". Much like my mile question, here you might ask the AI for factual information when you need a quick answer. Notably, everyone I talked to agreed that you would not use AI in this way when an important decision weighed on the answer. Proper research is still required for more weighty questions. One Digital Network Exploitation Analyst (DNEA) I talked to even made it a point to not ask an AI a question that could not be independently verified by a human.

Soldiers are also using AI for large, tedious tasks. Triaging data was often mentioned as an effective use case, as an AI can filter out a large amount of data that an analyst is not interested in reviewing. For example, an analyst might ask an AI to review a list of documents and return only the ones that contain the content the analyst is interested in. One Target Digital Network Analyst (TDNA) reported to me that using AI once reduced a pile of one-thousand documents to only ten documents, greatly reducing human work-hours. Cautious about missing potentially valuable data, he recommended that a human should look through all of the documents eventually anyway. But when time is short and answers are needed, AI can be a useful way to whittle down a workload.

One final use case that was often cited was using AI for language translation. One junior DNEA I interviewed was surprised by how well AI models could translate pictures with non-English text on them. But often the translations AI provides are not perfect. I spoke with a master linguist who stated that he will often ask AI to translate key terms related to a team's current target. He found that AI models will often struggle with idioms and colloquial phrases. For instance, a "script monkey," a term for a hacker who uses open-source capabilities, might be translated as a literal monkey—as an animal not an idea. He gets around this issue by sending out a list of common phrases and their translations to his team. That way, if any analysts are confused as to why the network security plan that they are reading involves real primates, for instance, they can refer to a master's translation.

Many Soldiers that I spoke to identified the importance of contextualization in an AI model—how well the model 'remembers' past queries and can understand a question from context. Some AI models struggled to associate a previously-asked question with a follow-up question, while others did very good job answering a question with very little context. Some Soldiers are experimenting with different models to see which ones best suit the work they need it to do. It seems as though Soldiers in the 782d MI Battalion are very aware of AI's limitation and how to best use AI models. As one Senior TDNA I interviewed put it: "[AI] is like your car, you know its drawbacks and how to overcome them. [You] understand where it performs well and where it doesn't." I have confidence that Soldiers in the Battalion are using AI wisely and productively. ■

The Force Multiplier: AI's Practical Integration into the Modern Army

By 2LT Nicolas Jimenez, 782d Military Intelligence Battalion (Cyber)

The integration of artificial intelligence into modern military doctrine is rapidly moving from a high-level strategic concept to a practical, operational reality. At the tactical level, where units and teams execute their missions, AI is now emerging as a powerful force multiplier, designed not to replace human ingenuity but to embolden it. This collaboration enhances the capabilities of service members by providing them with sophisticated and complex tools that increase their effectiveness. This allows for the streamlining of complex administrative and logistical tasks, freeing up personnel to focus on more of their critical duties. While in the cyber domain, it offers advanced analytical support to operators at the point of contact. By exploring these real-world applications, the value of AI reveals itself to be in its ability to empower our teams, making them more efficient, insightful, and resilient in an increasingly complex world.

Beyond the front lines, artificial intelligence is steadily reshaping the landscape for Soldiers across all specialties, automating the mundane and fortifying mission critical tasks. For those in the Cyber branch, AI acts as a vigilant digital guardian, continuously monitoring networks for anomalies, automating routine security protocols, and sifting through immense datasets to identify potential threats that a human analyst might miss. The time saved is then able to go right "back" to the Soldiers, freeing them to focus on higher-order tasks, such as proactive threat hunting and strategic defense planning. While at the same time, the average Soldier is beginning to experience the benefits of AI in their daily routines. AI driven systems are optimizing once tedious administrative duties, from managing supply requisitions to scheduling training, while also significantly reducing paperwork and improving efficiency. This allows Soldiers to dedicate more time to their core responsibilities, whether that is maintaining equipment, honing their Soldier skills, or preparing for their next objective. This ultimately fosters a more capable and focused force, ready to execute tasks and succeed in their efforts.

The Army's approach to training and professional development is also being fundamentally affected by AI, fostering a more adaptive and efficient learning environment. AI-driven educational platforms are moving the force beyond the traditional, one-size fits all classroom by creating personalized learning experiences for each Soldier. By identifying individual strengths and weaknesses, these systems can deliver targeted instruction, ensuring a deeper and more lasting understanding of complex material. In addition, AI is revolutionizing practical training by creating highly realistic and dynamic simulations that can adapt to a Soldier's actions, presenting unpredictable challenges which then elevate critical thinking and decision-making skills in a way never seen before. The time saved through this approach is significant; by automating routine assessments and optimizing learning schedules, Soldiers can master new skills more rapidly, allowing them to return to their units faster and better prepared for the complexities of the modern battlespace.

In conclusion, the integration of artificial intelligence is proving to be a pivotal moment for the armed forces, impacting everything from daily administrative burdens to the strategic complexities of cyber defense and the traditional Soldier training. The consistent theme is one of enhancement; AI is making our units more efficient, our training more effective, and our Soldiers better prepared. By handling computational and repetitive loads, these systems are elevating the role of the individual service member, allowing them to dedicate their focus to critical thinking, adaptability, and leadership that no machine can replicate. As this technology becomes ever more integrated within our day-to-day operations, the ultimate measure of our strength will not be the sophistication of our algorithms and tools, but the ingenuity of the Soldiers who wield them.

Reference:

Marine Corps Staff. (2025, May 2). Inaugural Marine Corps AI fellowship advances workforce applications. Department of War. https://www.war.gov/News/News-Stories/Article/Article/4394411/inaugural-marine-corps-ai-fellowship-advances-workforce-applications/

Pfaff, C. A. (2023, May 10). AI's growing role in command and control. U.S. Army War College War Room. https://warroom.armywarcollege.edu/articles/ais-growing-role/

Stieglitz, C. J. (2024, January 26). Artificial intelligence as a combat multiplier: Using AI to unburden Army staffs. Military Review. https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/AI-Combat-Multiplier/

The End of the World as We Know it: AI Shaping How We Produce Code

By CPT Kenneth McGaffey, Operations Support Element

The increasing ubiquity of large language models (LLMs) affects many code developers. Within the Cyber Solutions Detachment (CSD), LLMs represent both opportunity and uncertainty. This article will explore how many tasks developers have become accustomed to will be replaced by AI. However, new opportunities exist with this increased productivity as a force multiplier.

THE RAPID advancement of Large Language Models (LLMs) such as ChatGPT and GitHub Copilot has fundamentally changed the way software is written. What began as simple autocomplete tools have evolved into systems capable of generating full applications, debugging complex errors, refactoring legacy code, and even deploying software autonomously. As AI agents become more capable of planning, reasoning, and executing multi-step workflows, a pressing question emerges: will LLMs and AI agents replace the cyber capabilities developer (CCD) altogether?

There are compelling reasons to believe that many traditional developer roles will significantly diminish. First, LLMs dramatically reduce the cost and time required to produce functional software. Tasks that once required hours of manual implementation (i.e. writing boilerplate code, building APIs, generating unit tests, etc.) can now be completed in minutes. For the Cyber Solutions Development (CSD) detachments, this means fewer junior level developers are needed to perform repetitive or well-defined tasks. Basic developers are especially vulnerable because much of their work involves structured, predictable problem-solving; precisely the domain where LLMs excel.

Second, AI agents are moving beyond passive code generation toward autonomous execution. Modern agent frameworks can read documentation, search repositories, write code, run tests, interpret failures, and iterate until success. When connected to deployment pipelines and cloud platforms, these systems can ship production-ready features with minimal human intervention. As reliability improves, the economic incentive to automate grows stronger, even within the CSD. CSD is incentivized by efficiency, and if AI agents can deliver software faster and cheaper than crews of developers, work role reductions become a rational outcome.

Third, software development itself is becoming more abstract. Historically, programming required detailed knowledge of syntax, memory management, and system architecture. Today, high-level frameworks and cloud platforms have already automated much of that complexity. LLMs accelerate this trend by allowing developers to describe desired functionality in natural language. In this paradigm, coding shifts from writing precise instructions to specifying intent. If intent specification becomes simple enough, fewer specialized developers may be required.

However, full replacement is not a certainty. Coding is not merely typing syntax; it is problem formulation, system design, trade-off analysis, and understanding ambiguous human requirements. LLMs are powerful pattern predictors, but they lack genuine comprehension, long-term accountability, and context awareness. AI agents may produce code, but they do not bear responsibility for security vulnerabilities, compliance risks, or architectural decisions that could cost millions. Human oversight remains critical, particularly in high-stakes domains.

Moreover, the integration of LLMs and AI agents means the CSD will rely even more on senior developers than before. Senior developers must start somewhere; that somewhere is basic development. The training pipeline for seniors relies on accepting basic developers. If the CSD removes the basic developer work role, the senior developer work role is to follow. Trained and capable senior developers will continue to be a priority even with AI advancements.

What is more, technological revolutions historically reshape labor rather than eliminate it entirely. The rise of compilers did not eliminate programmers; it changed assembly programmers into higher-level software engineers. The emergence of cloud computing did not remove IT professionals; it transformed them into DevOps engineers and cloud architects. Similarly, LLMs will likely not eliminate CCDs, but instead redefine them. Developers may shift from manual coding toward supervising AI agents, validating outputs, refining prompts, designing architectures, and integrating AI into products.

Ultimately, LLMs and AI agents are likely to replace certain developer tasks and reduce demand for routine programming roles, particularly at the junior level. However, complete replacement of the CCD is unlikely in the near term. Instead, the CSD will likely undergo a structural transformation. The developers who thrive will not compete with AI at writing boilerplate code; they will leverage AI as an amplifier of productivity and focus on higher-level thinking. The future of developers may belong not to those who type the fastest, but to those who best collaborate with intelligent machines. ■

Coffee is No Longer the Only Productivity Tool

By SPC Dawson Mayernik, Operations Support Element

Artificial Intelligence as a Force Multiplier: Enhancing Productivity Across HHC and

IN TODAY'S OPERATIONAL ENVIRONMENT, Army units are expected to accomplish more in less time and with fewer resources. Administrative tasks continue to increase, the time for reporting decreases, and leaders at every level are faced with the challenge of executing their mission while dealing with a growing list of complex tasks. During these challenges, Artificial Intelligence (AI) has appeared as a tool that increases productivity and performance at Headquarters and Headquarters Company (HHC) and staff sections.

Instead of being a replacement for leaders or staff professionals, AI is a force multiplier that removes administrative obstacles and allows leaders and Soldiers to focus on what matters most: readiness and success.

The Administrative Reality of Modern Units

The staff sections are the engine of effectiveness for any organization. From personnel decisions and evaluations to training and operations, HHC and the primary staff sections of the command are responsible for ensuring that the commander's intent is carried out.

However, much of this effort is formatting-intensive, repetitive, and time-sensitive. Leaders spend countless hours writing memorandums, updating training trackers, reading regulations, creating briefing slides, and answering higher headquarters requirements. While these are important, they also take time away from mentorship, training oversight, and leadership.

AI applications are poised to help in this kind of environment. By taking the repetitive work of writing, organizing information, and creating formatted versions of text, AI applications can save time and effort without sacrificing quality.

Enhancing Personnel and Administrative Efficiency

In the S1 and training room community, efficiency and precision are paramount. Personnel actions, awards, evaluations, and counseling statements are subject to rigorous regulatory requirements and formatting specifications. Even small discrepancies can cause processing delays and unnecessary consternation.

AI can help with:

- Writing memorandums for record (MFRs)
- Writing counseling statements in regulatory speak
- Creating award bullet statements from performance data
- Condensing essential guidance from Army regulations
- Formatting documents to regulatory specifications

Rather than starting from scratch, personnel can begin with an organized draft and use professional judgment. This cuts preparation time dramatically while enhancing clarity and consistency.

AI can also help with reviewing documents for grammar, tone, and formatting, which encourages professional communication and minimizes the need for revisions.

The result is not automated accountability, but rapid action.

Improving Operational Planning and Staff Coordination

The challenge for operational staff sections is different: turning guidance into doable plans. Whether writing an operations order (OPORD), creating a training schedule, or creating a risk assessment, staff officers and NCOs must synthesize a lot of information in short order.

AI can help in this process by:

- Organizing OPORD templates
- Creating initial risk assessment frameworks
- Creating synchronization matrices
- Summarizing higher headquarters guidance
- Creating briefing or rehearsal outlines

By quickly organizing information, AI cuts the time needed to create planning products from scratch. Staff sections can then concentrate on analysis, coordination, and planning instead of formatting.

Leaders maintain complete authority for validation and approval, but they get their time back.

AI as a Force Multiplier; Not a Replacement

AI does not displace leadership, decision-making, or professional military judgment. AI cannot interpret the commander's intent, understand unit culture, or evaluate mission context.

AI helps with structure, writing, and summarization. Not decision-making.

Leaders retain responsibility for accuracy verification, regulatory compliance, and critical thinking. When used prudently, AI multiplies effectiveness. When used recklessly, AI introduces risk.

The human element remains decisive.

Measurable Productivity Gains

The advantages of AI integration within staff sections are clear.

1. Reduced Drafting Time
   Activities that took several hours of formatting and initial writing can now be initiated in minutes with an organized product.
2. Improved Standardization
   AI promotes uniform formatting and proper language use, raising the standard of unit correspondence.
3. Faster Reporting Cycles
   Standard reports and administrative messages can now be generated

more quickly, allowing for swift transmission to commanders.

4. Increased Leader Availability With less repetitive administrative work, leaders can now have more time for training, counseling, and preparing for missions. Boosted productivity is a direct contributor to readiness.

Responsible Integration and Considerations

Although the benefits are well understood, it is important to responsibly integrate AI. Units must be able to handle sensitive, classified, and personally identifiable information (PII) in accordance with Army policy and cybersecurity regulations.

Leaders must ensure:

- Classified or controlled information is not entered into unauthorized systems
- AI-generated content is verified before formal use
- All regulatory requirements are met
- Soldiers understand both the capabilities and limitations of AI

AI literacy should be considered a skill for professional development. Leaders who understand how to effectively use AI can maximize the benefits while minimizing the risks.

Looking Ahead: AI and the Future of Staff Work

As the Army presses on with its digital transformation, AI is likely to be further woven into the fabric of enterprise systems. Predictive readiness analytics, automated reporting dashboards, and smart planning tools could become the norm in staff operations.

This is an opportunity for HHC and the primary staff sections. By using AI in a responsible way, units can cut administrative work, enhance communication, and improve performance.

Administrative efficiency is key to operational success. When everyday tasks are simplified, leaders can devote more of their time and effort to training Soldiers, developing teams, and accomplishing the mission.

Conclusion

Artificial Intelligence is not an idea for the future, but it is a current capability that increases the productivity of Army staff sections. In the HHC and administrative environment, AI eliminates the repetitive task, speeds up the planning cycle, and improves the quality of the documents.

Most importantly, it gives back time to the leadership.

When used properly and managed by professionals, AI is a force multiplier that enhances readiness and performance. The Army has always been able to adapt to new technologies to keep its edge. AI is the next step in this tradition. ■

The Impact of Russian and Chinese Artificial Intelligence on the American Cyber Domain

By CPT Ty Wolfenbarger, 11th Cyber Warfare Battalion

EVOLUTION IS A NOTABLE CHARACTERISTIC of the cyber domain; rapid digitization of infrastructure grows the attack surface of networks faster than the development of measures to protect data. There is an ever-present race condition between cybersecurity defenders and adversaries who aim to damage, degrade, or steal information (Baidu, 2023). The war for cyberspace is determined by the entity that can most effectively complete cyber operations and stay competent in the latest practices. Artificial Intelligence (AI) is a growing technology that can benefit offensive and defensive cyberspace activities by reducing the time and resource strain required to analyze and use the exponentially growing data created daily. The purpose of this paper is to forecast the potential impacts that Russia and China could impose on the United States in the cyber domain by discussing the current state of information warfare (IW) and AI, the various goals of the three nations, examples of each nation using AI, and actions the U.S. can take to improve the outcome of continuous cyber conflict.

Information Warfare and Artificial Intelligence

The information environment (IE) is a broad concept including all individuals and systems that collect, process, or use information in any of its dimensions. The United States recognizes three dimensions of the informational environment: the physical, informational, and cognitive dimensions (Hunter, 2023). IW is any act by one party aiming to deliberately manipulate information in any dimension to influence a choice or decision for military or strategic gain. IW occurs primarily through two means information warfare and influence operations (IWIO) and cyber-enabled influence operations (CEIO). IWIOs are the specific actions an entity packages together to influence an intended target, while CEIOs are a subset of IWIO that utilizes elements of cyberspace to influence a target (Hunter, 2023). IWIO focuses mostly on the cognitive dimension to define success; CEIO is associated with the physical dimension through Electromagnetic Warfare (EW) and the information dimension through Cyber. AI can amplify either of the listed operations by adding intelligence to shape an operation's narrative to increase success.

AI is any software program that can execute tasks that mimic human qualities in areas such as spatial perception, audio, text, decision-making, and learning (Hunter, 2024). There is little research generated on how the major powers around the globe will implement AI in IWIO, but it represents a growing consideration for all states' security strategies. China, Russia, and the U.S. have already utilized the power of AI to influence narratives, national stability, international alliances, and the survivability of governments (Hunter, 2023). This section focused on how AI can influence IE and introduced the significance of implementing it within IWIO conducted by nation-states.

China, Russia, and U.S. Goals in the Information Environment

AI implementation for IWIO will vary based on the strategic goals and appetite for use between nations; these goals are heavily based on the governance model the nation supports (Svenmarck, 2019). The common benefits of AI concerning IE heavily relate to the increased speed of creating and analyzing data to determine improved information for tactical and strategic decisions. A major characteristic of AI is the ability to offset resource and technology deficiencies; the Chinese call this concept asymmetric warfare (Hunter, 2024). The final commonality of AI between all nations is an infinite information operation feedback loop; AI creates information and effects that can be used for additional fallow-on operations. China, Russia, and the U.S. take advantage of all these concepts to some degree.

China's IW strategy is influenced by its authoritarian government; they believe IW should focus on the three warfare models: legal, psychological, and media. China's whole-of-society approach allows for expedited action and aggressive collection of information on its domestic and foreign audiences. China conducts both grey-zone activities, actions below kinetic conflict, and surveillance capitalism (personal information obtained and then sold by private organizations (Hunter, 2023)). China specializes in the use of surveillance capitalism-driven operations to spread disinformation and propaganda to create problems for adversaries. This is critical for the U.S. Department of Defense (DOD), specifically entities like the Army Cyber Branch, because China views the environment as a persistent offensive engagement with its peers. The strategic goal for China is to increase influence operations to weaken adversary states and spread digital authoritarianism through diplomatic/economic activities, such as the Belt and Road initiative (Hunter, 2023). AI is significant in this goal at the tactical level because it allows them to compete in areas of overmatch with the U.S.

Russia's IE strategy has identical elements to China's because of similar government sentiments when implementing AI. The Russian government freely targets foreign and domestic populations when collecting information that garners support through narratives made with AI. Many experts think Russia lags both the U.S. and China in the field of AI, but their willingness to utilize it for disseminating propaganda surpasses both states. The major drawback to Russia's use of AI is the reliance on Western states for

AI development and innovation. Russia is more aggressive when it comes to the physical and cognitive use of CEIO and believes in constant warfare with the U.S. targeting socio-political division in the American IE with deep fake propaganda and allies of Ukraine with EW capabilities (Hunter, 2024). These activities directly align with their strategic IWIO goals to disrupt the spread of Western ideology threatening the current regime. This straightforward goal and decisive actions give the DOD and the Army Cyber Branch clear expectations and indicators of Russian-sponsored operations and potential end-states.

The U.S. is the polar opposite when it comes to its stance on IWIO activities and the use of AI during an operation. The US's western ideals and democratic system of governance limit the DOD's ability to collect and use information, especially the domestic information of the citizens it is entrusted to protect. The U.S. only utilizes aggressive tactics in a war-time environment, limiting the ability to compete in the global IE. AI is seen as an amplifier instead of a built-out capability; this technology is used defensively and not as a tool to gather and weaponize information (Wilson, 2019). The U.S. focuses on AI to detect indicators of attack and discredit disinformation; the U.S. has an estimated 48 hours to disprove false narratives before they receive creditability to the intended target (Heslen, 2020). The DOD and the Army Cyber Branch will need to consider these limitations and improve them as AI becomes more dominant in the global IE.

China, Russia, and U.S. AI Implementation

Overall, Russia and China can aggressively collect data to implement AI tools which allows them to push information and gray-zone operations. These continual operations make the nations more effective in combating the U.S. on multiple fronts. This section will focus on Chinese and Russian IWIO that utilizes AI to stress the gap between the U.S. and its adversaries; the areas of improvement for the DOD and Army Cyber Branch will be apparent based on the discussion.

China's most notable IWIO from a strategic point of view is the influencing actions in Taiwan and the South China Sea. China has been successful and uncontested in the media domain of the region through astroturfing, the creation of artificial ideas to popularize a narrative, and complex botnets to control the cognitive dimension in the region. Common narratives that the Chinese have been able to manipulate include painting democracy-supporting Hong Kong citizens as violent extremists, validating unlawful claims to Taiwan and the South China Sea, and misrepresenting intentions of the U.S. inhabitation with partner nations (Hunter 2023). These observances of information manipulation provide a dual benefit to China by synthesizing unproven narratives that support the growth of digital authoritarianism and indirectly attack the region's mindset of the American way of life with little hindrance from the U.S. point of view. The U.S. Military and the Army Cyber Branch should coordinate with national policy and authorities to counter adversarial IWIO campaigns in the region to combat China's actions in the information dimension before it becomes irreversible.

Open-source reporting and U.S. assessments have documented foreign IWIO targeting U.S. electoral processes. The IWIO campaign dates back years before the observed interference operations and utilized many forms of information influencing actions. Russia, Iran, and other actors attempted to create or created physical activities in the form of staging counter-protests to sow discord between competing ideologies leading into the election. Another format of "fake" news that adversaries were able to create was forging documents by stealing real campaign forms and editing them to influence voters' thoughts (Hunter, 2023). The onslaught of fake news formats was a significant concern in the legitimacy of election results and showcased adversaries' ability to successfully outcompete DOD's and by extension Army Cyber Branch's information protection measures.

Areas of Improvement for the U.S. in AI

The Army Cyber Branch and the U.S. Military should first work to improve the security of its information within its domestic borders, then improve the process to counter peer adversary IWIO through its counter-influence operations from the social media perspective. The current IWIO national strategy is incomplete because it lacks centralization and unity; the DOD is attempting to fix this issue through network convergence (Wilson, 2019). Network convergence will improve communication between services and partner environments by providing common definitions across the organization and data normalization to better manage actions related to data. Additionally, information security could better stabilize with the assignment of a responsible organization to manage the various components of IWIO. Overall, the U.S. has increased the budget for information-related assets by $20 million to compete with Russia and China in the environment, but it was used for more defensive AI and cloud-related technology (Hunter, 2024). A portion of that budget should aim to reduce China's and Russia's effectiveness in the domain from a technical perspective. Currently, the U.S. has relied on logistic and economic material acquisition to limit the growth of China's influence; there comes a point where the inability to amplify the U.S. narratives will become an issue if competition escalates to conflict (Wilson, 2019).

Conclusion

In conclusion, the increased growth of data creates a challenge for information security that requires innovative technologies, like AI, to properly secure. AI provides a benefit to both offensive and defensive aspects of information security. A nation's characteristics, such as government structure and relationship with its citizens, significantly effect the method of utilizing AI. Russia and China have whole-of-society approaches and view the IE as a constant domain of contention; this allows them to outcompete the U.S. in both IWIO and CEIO functions. The AI-enabled influence operations in Taiwan

and the South China Sea show that the U.S. needs to coordinate with national policy and authorities to counter-influence operations; while the election interference show that the U.S. is not ready to combat complex IWIO activities. The primary shortfalls for the U.S. in the field of IWIO and CEIO relate to failure to properly communicate and coordinate actions in the domain; additionally, more resource provisions should be allocated to counter-influence operations if the U.S. and Army Cyber Branch hope to be competitive in global strategic objectives related to IWIO.

Reference:

Badiu, M., & Tica, L. (2023). The Complexity of the Current Operational Environment and the Military Leader's Ability to its Ongoing Challenges. International Conference Knowledge-Based Organization, 29(1), 12-16, https://doi.org/10.2478/kbo-2023-0003

Heslen, J. J. (2020). Neurocognitive hacking. Politics and the Life Sciences, 39(1), 87–100. https://doi.org/10.1017/pls.2020.3

Hunter, L. Y., Albert, C. D., Henningan, C., & Rutland, J. (2023). The military application of Artificial Intelligence Technology in the United States, China, and Russia and the implications for global security. Defense and Security Analysis, 39(2), 207–232. https://doi.org/10.1080/14751798.2023.2210367

Hunter, L. Y., Albert, C. D., Rutland, J., Topping, K., & Hennigan, C. (2024). Artificial Intelligence and information warfare in major power states: How the US, China, and Russia are using artificial intelligence in their information warfare and influence operations. Defense and Security Analysis, 1–35. https://doi.org/10.1080/14751798.2024.2321736

Svenmarck, P., Loutsinen, L., Nilsson, M., & Schubert, J. (2019). Possibilities and Challenges for Artificial Intelligence in Military Applications. *Swedish Defense Research Agency*

Wilson, N. (2020, August 3). Understanding the battle for AI in warfare through the practices of assemblage: A case study of project maven. Utrecht University Student Theses Repository Home. https://studenttheses.uu.nl/handle/20.500.12932/37392

How AI is Empowering Our HQ and Battalion Staff

By 1LT Abdiel Compres, 11th Cyber Warfare Battalion

IN CHARLIE COMPANY (CHAOS), AI tools are proving to be a significant force multiplier, enhancing both administrative and operational efficiency. These advancements are freeing up our personnel from menial tasks, allowing them to focus on more critical, high-value work and better support our soldiers..

Streamlining Administrative Burdens

One of the most immediate impacts of AI is cutting through the daily administrative workload. By handling routine clerical and preparatory duties, AI allows leaders to reclaim valuable time that would otherwise be spent between long meetings and tedious tasks.

AI Application	Benefit
Document & Template Creation	Instantly formatting Word documents for Memorandums for Record (MFRs) or creating complex Excel sheet templates for Company Budget meetings saves hours of manual work.
Evaluation Support	AI assists in finding specific, impactful wording for OERs and NCOERs, helping leaders accurately articulate performance and potential without getting bogged down in wordsmithing.
Automated Notetaking	AI scribes can transcribe meetings and generate summaries, significantly reducing the time spent on documentation and allowing personnel to be more engaged during discussions.

Enhancing Operational & Strategic Effectiveness

Beyond administrative support, AI is having a profound impact on our operational and strategic capabilities. It helps us think more abstractly about problems without getting caught up in the finer details that can be fleshed out later.

AI Application	Benefit
Creative Brainstorming	AI is an excellent partner for brainstorming ideas for Leader Professional Development (LPDs), providing a foundation of concepts that leaders can then refine and tailor.
Resource Discovery	AI can quickly find resources, regulations, and publications that a leader might not have known about, becoming an essential tool for research and problem-solving.
Decision Support	AI algorithms can analyze complex datasets to identify patterns and provide data-driven recommendations, enhancing strategic decision-making under pressure.

A Partnership for Deeper Thinking

It is crucial to view AI not as a replacement for critical thinking, but as a powerful asset that enhances it. This new tool allows leaders to get to the heart of an issue more efficiently. It is akin to how the calculator does not take away from the foundational skills needed for mathematics but helps save time by getting to the bottom line in a more efficient manner. ■

Secretary of the Army Reviews Future of Cyber Warfare, AI Integration at ARCYBER

By SSG DeMarco Wills, U.S. Army Cyber Command

FORT GORDON, GA.- The U.S. Secretary of the Army visited U.S. Army Cyber Command (ARCYBER) leaders at Fort Gordon, March 26.

During the visit, the Honorable Dan Driscoll engaged with ARCYBER commander LTG Christopher L. Eubank, other senior leaders, and operators to discuss the future of cyber warfare and its integration with the total force.

As part of these discussions, Eubank briefed Driscoll on the command's role in delivering lethality and readiness for the U.S. Army in the cyber domain.

Our role is to seamlessly integrate cyberspace operations, information operations, and electronic warfare to provide commanders at every echelon with a full spectrum of capabilities," said Eubank. "We are constantly adapting and modernizing to ensure that our forces at the tactical edge are equipped to fight and win in a complex, data-driven environment. We know we are ready for conflict because we conduct our mission against the enemy every day."

In addition to meeting with ARCYBER leaders, Driscoll also met with the science advisor to the ARCYBER commanding general, Mark "Al" Mollenkopf, who briefed him on optimizing military missions and staff effort through automation and artificial intelligence.

"ARCYBER is leading the Army's effort to apply AI to cyberspace operations," said Mollenkopf. "Our focus is on leveraging artificial intelligence for our warfighters that creates a powerful force multiplier. By automating routine tasks and analyzing vast amounts of data, we empower our soldiers to make faster, more informed decisions, ultimately enhancing mission effectiveness

and safeguarding our nation's interests in the digital domain."

During the visit, ARCYBER demonstrated offensive and defensive capabilities to Driscoll. The 11th Cyber Warfare Battalion, the Army's first expeditionary cyber battalion, conducted RF-enabled cyber operations using unmanned aerial systems.

These engagements underscore how the U.S. Secretary of the Army's visit highlights the growing importance of cyberspace operations, especially the defense of critical infrastructure, to the Army's readiness and modernization priorities.

The Secretary's visit affirmed ARCYBER's role in driving Army modernization. Demonstrations, from AI analysis to unmanned aerial operations, showed a command both preparing for and shaping the future of warfare. This engagement underscores the Army's commitment to investing in cyber capabilities, ensuring national security and a decisive global edge.

Secretary of the Army ARCYBER Visit

FORT GORDON, Ga. – U.S. Secretary of the Army Dan Driscoll met with the command team for the U.S. Army Cyber Command March 26, 2026.

LTG Christopher L. Eubank, commanding general of ARCYBER, and CSM Jebin Heyse, ARCYBER's senior enlisted leader, met with the Army Secretary to brief him on ARCYBER's role in delivering lethality and readiness for the U.S. Army.

(U.S. Army photos by SSG DeMarco Wills)

Brigade Competitive Cyber Team Excels at 10th Annual SANS Services Cup

WASHINGTON – The 780th Military Intelligence Brigade (Cyber) competitive cyber team, the Speculatores, placed second out of 10 competing Department of War teams at the 10th Annual SANS Services Cup, December 15.

According to the SANS Institute strategic accounts manager for the U.S. Army this was an "incredible" feat for our new team because several other service teams competed before, including the Army National Guard team who regained the Cup for the fifth time out of the last six Services Cup.

Their second place finish also gives the Army Speculatores team a slot in the SANS International Cup in 2026 – an opportunity to compete against government organizations all over the world.

To round out the top five U.S. Space Forces took third, U.S. Air Force Reserve fourth, and a U.S. Air Force team took fifth. The Speculatores team lead said this SANS Services Cup competition was "heavy with AI, forensics, and social engineering." The next major event for the team will be the upcoming President's Cup competition in February.

Going into its second year, the brigade team uses the CISA led and hosted President's Cup Cybersecurity Competition 7 to determine the primary team members. Registration for that competition is open now at https://www.cisa.gov/presidents-cup-cybersecurity-competition. There is also a practice area at https://pccc.cisa.gov/gb/practice.

Brigade Soldiers and Civilians interested in trying out for the Speculatores should contact the brigade's public affairs officer at usarmy.meade.780-mi-bde.list.780th-mi-bde-pao@army.mil.


MISSIONE
PC07

Praetorians Compete in CISA President's Cup Cybersecurity Competition

By the Public Affairs Office, 780th Military Intelligence Brigade (Cyber)

WASHINGTON – Soldiers of the 780th Military Intelligence Brigade (Cyber), Praetorians, competed in the seventh annual Cybersecurity & Infrastructure Security Agency (CISA) 2026 President's Cup Cybersecurity Competition (PC7) to identify, recognize, and reward the best cyber talent across the federal workforce.

According to the CISA PC7 website, the competition is "designed around realistic scenarios tied to critical NICE (National Initiative for Cybersecurity Education) Framework roles and includes individual tracks (defensive or offensive) and a team track for groups of two to five."

Since 2019, select Praetorian Soldiers and Civilians have competed in the annual event, and following the first two virtual rounds – we are happy to announce – the brigade will have representatives in both the individual and team in-person finals held in April.

Congratulations to Mr. Robert Ighnat, SSG Robert Meyers Jr., 1LT Osho Yonzon, and LTC Michael Kranch, who all qualified for the individual finals to be held April 14, defensive track; and April 15, offensive track. Of note, LTC Kranch qualified for both tracks.

Although the brigade's competitive cyber team, The Speculatores, did not advance, a team consisting of MAJ Steve Rogacki, 780th MI Brigade, and brigade alumni: Army Reservist CPT Brian Welch, CPT Jinny Yan, MAJ Ben Allison, along with their fifth team member, Marine Corps Maj. James Russell, did qualify for the teams' competition to be held on April 16.

Mr. Ighnat, a Department of the Army Civilian with the Operations Support Element, 780th MI Brigade, is moving on to the individual finals; however, he also competed in the teams' event as a member of the five-person brigade competitive cyber team, The Speculatores.

"I compete in the President's Cup because I enjoy doing Cyber CTF (capture the flag) events and the ones hosted by CISA's Presidents Cup team are not only fun but also challenging," said Ighnat. "These competitions are a great way for me to keep my skills sharp and make myself aware of different and new technologies or techniques. The critical thinking required to tackle these problems are another way to keep me agile. Both reasons are directly related to my job as a cyberspace operator which is always a positive."

U.S. federal civilian employees and uniformed military personnel, including those on active duty and in the reserves, are eligible to participate either individually, as members of a team, or in both capacities. The competition has two virtual qualifying rounds; top scorers must attend the in-person finals in the National Capital Region.

"The advice I would give others competing next season is that if you hit a roadblock the best thing you can do is take a minute to breathe and then step back through your process. A lot of times you might have missed a key piece of data in your prior tasks. In so doing, this allows you to re-confirm your work and give you some time to re-think your strategy," said Ighnat. "Additionally, time management is key. Knowing when to cut your losses and move on to another challenge is a great strategy because when we tackle a problem we want to solve it regardless of how long it takes and during these time-limited competitions that can be your downfall."

For more information on the event visit the CISA PC7 website at https://www.cisa.gov/presidents-cup-cybersecurity-competition.

"Ubique Et Semper In Pugna"

"Everywhere and Always…In the Fight!"

11th Cyber Warfare Battalion Executes Hellhound Week to Sharpen Warrior Skills

By CPL Teanna Dooley, public affairs liaison, 11th Cyber Warfare Battalion

FORT GORDON, GA. – Soldiers from Headquarters and Headquarters Company (HHC), 11th Cyber Warfare Battalion, Hellhound, conducted Hellhound Week to demonstrate their commitment to readiness, discipline, and warrior proficiency, February 4 and 5.

The training event was as a comprehensive assessment of Soldiers' Level 10 Warrior Tasks and Battle Drills that align with the company's Mission Essential Task List (METL) and Expert Soldier Badge (ESB) standards.

According to the operations plan, Hellhound Soldiers were challenged throughout the week across a wide spectrum of tactical and technical tasks designed to reinforce core Soldier competencies.

During the day land navigation event Soldiers were required to locate four out of four points within a time constraint. The exercise tested not only map-reading and terrain association skills but also individual confidence and resilience under pressure.

Soldiers also executed Battle Drill 1A: React to Contact, a cornerstone of small-unit tactics. Teams maneuvered through tactical formations, negotiated linear danger areas, and practiced lift-and-shift fire techniques while responding to simulated enemy contact. This drill emphasized communication, teamwork, and rapid decision-making.

Weapons proficiency was another key focus area. Soldiers disassembled and reassembled the M4 carbine, M249 and M240 machine guns reinforcing their understanding of weapon function, maintenance, and safe handling critical skills for any operational environment.

Technical proficiency was equally prioritized. Participants conducted Preventive Maintenance Checks and Services (PMCS) on military equipment and completed DA Form 5988-E to document faults and verify operational readiness. This reinforced the importance of equipment accountability and maintenance discipline within the formation.

Communications tasks added another layer of complexity. Soldiers operated the AN/PRC-1523D SINCGARS radio, loading single-channel plain text, performing communications checks, and transmitting a 9-Line MEDEVAC request. These tasks ensured that every Soldier could establish reliable communications in both routine and emergency scenarios.

Explaining the significance of Hellhound Week, CPT Cutosha Dilworth, the HHC Hellhound commander stated, "Leading this unit has been the greatest honor of my life, witnessing a spirit forged in the mud and adversity we faced together."

Dilworth emphasized that Hellhound Week is not only a test of skill and readiness, but a reminder of the family-like bond that exists within the company.

"Hellhound Week showcased the professionalism and adaptability of HHC Soldiers," said Dillworth. "The training not only validated individual and collective readiness but also strengthened the company's ability to support the broader mission of the 11th Cyber Warfare Battalion."

As the Army continues to evolve in a rapidly changing operational environment, Dilworth remarked that she and her team remain committed to "building agile, lethal, and technically proficient Soldiers."

FORT GORDON, Ga. – Soldiers from Headquarters and Headquarters Company (HHC), 11th Cyber Warfare Battalion, Hellhound, conducted Hellhound Week to demonstrate their commitment to readiness, discipline, and warrior proficiency, February 4 and 5.

The training event was as a comprehensive assessment of Soldiers' Level 10 Warrior Tasks and Battle Drills that align with the company's Mission Essential Task List (METL) and Expert Soldier Badge (ESB) standards.

U.S. Army photos by SFC James McBride, SSG Laun Fountain, and SFC Kyle Singleton ■

11th Cyber Warfare Battalion Best Squad

FORT GORDON, Ga.. – Soldiers from the 11th Cyber Warfare Battalion (Leviathan) competed in their battalion-level Best Squad Competition (BSC), February 17 to 20, to determine which squad will represent the Leviathans at the U.S. Army Cyber Command BSC later this year.

According to the Army Best Squad website at https://www.army.mil/bestsquad/, the competition assesses "each squad on their technical and tactical proficiency, as well as their ability to work as a disciplined and cohesive team."

The competition features "a multitude of different fitness and combat related events ranging from an official fitness assessment and various weapons lanes to a strenuous 12-mile foot march and detailed individual warrior tasks and squad battle drills."

Each squad consists of five Soldiers: a squad leader, which is a sergeant first class or staff sergeant; a team leader, which is sergeant or corporal; and three squad members in the ranks of specialist or below.

Global Reach, Global Impact!
"Everywhere and Always…In the Fight

Vanguard Sweeps the Brigade Best Squad Competition

By the Public Affairs Office, 780th Military Intelligence Brigade (Cyber)

FORT A.P. HILL, VA. – Soldiers representing three of the four battalions under the command of the 780th Military Intelligence Brigade (Cyber), Praetorians, competed in the brigade's 2026 Best Squad Competition (BSC) March 2 through 6.

Soldiers from the 781st MI Battalion (Vanguard); 782d MI Battalion (Cyber Legion); and the Operations Support Element, competed to represent the Praetorians at the U.S. Army Intelligence and Security Command BSC, April 15 to 21.

The brigade's fourth battalion, the 11th Cyber Warfare Battalion (Leviathan), completed their BSC in February and will represent the Leviathans at the U.S. Army Cyber Command BSC later this year.

According to the U.S. Army Best Squad website (https://www.army.mil/bestsquad/), the competition assesses "each squad on their technical and tactical proficiency, as well as their ability to work as a disciplined and cohesive team."

The competition features a multitude of different fitness and combat-related events ranging from an official fitness assessment and various weapons lanes to a strenuous 12-mile foot march and detailed individual warrior tasks and squad battle drills.

Each squad consists of five Soldiers: a squad leader, which is a sergeant first class or staff sergeant; a team leader, which is sergeant or corporal; and three squad members in the ranks of specialist or below.

"This was a challenging and demanding event that tested the participants' mental, physical, and tactical readiness," said CSM Joseph P. Daniel, Praetorian 7, the senior enlisted leader for the 780th MI BDE. "All competitors demonstrated the highest levels of professionalism and represented their battalions with distinction."

On behalf of COL Candy Boparai, the brigade commander; CW4 Chad Mastbergen; Mr. Aaron Tipton, the brigade's senior civilian advisor, and CSM Daniel, the Praetorians are pleased to announce the winners of the brigade's 2026 Best Squad, Noncommissioned Officer (NCO) and Soldier of the Year Competition.

- Brigade 2026 Best Squad: 781st MI Battalion: SSG Joshua Vanbuskirk; SGT Ángel Jesús Martinez; SPC Mark Whitley; SPC Jovi Acasio; and SPC Kiari Amerson
- Brigade 2026 NCO of the Year: SSG Vanbuskirk, 781st MI Battalion
- Brigade 2026 Soldier of the Year: SPC Amerson, 781st MI Battalion

The Vanguard Best Squad mentor, SGT Ethan Davis, said the slogan for the squad members was "Suck Less."

"This saying was frequently quoted throughout the training process to all Soldiers. The saying stems from the other side of 'do better,'" said SGT Davis. "The reasoning behind the change in saying is because you can only get so much better at an individual task; however, every time you do something you always suck less at it… Suck Less."

Please pass on your congratulations to these outstanding Soldiers and NCOs of the 781st on their significant achievement of winning the Brigade Best Squad Competition.

"Ubique Et Semper In Pugna"

"Everywhere and Always…In the Fight!"

780TH MILITARY INTELLIGENCE BRIGADE (CYBER)

2026
BEST SQUAD OF THE YEAR

SSG JOSHUA VAN BUSKIRK; SGT ÁNGEL JESÚS MARTINEZ;
SPC MARK WHITLEY; SPC JOVI ACASIO; AND SPC KIARI AMERSON

PRAETORIANS

780TH MILITARY INTELLIGENCE BRIGADE (CYBER)

2026

NCO OF THE YEAR

SSG JOSHUA VAN BUSKIRK

780TH MILITARY INTELLIGENCE BRIGADE (CYBER)

2026

SOLDIER OF THE YEAR

SPC KIARI AMERSON

780TH MI BDE BEST SQUAD COMPETITION

PRAETORIANS

780TH MI BDE BEST SQUAD COMPETITION


BRAVO
U.S. ARMY
DO
U.S. ARMY
HOANG
U.S. ARMY
JONES
U.S. ARMY
NEWLAND
U.S. ARMY

Army Transitioning to Support Deep Sensing in Multidomain Operations

By MSG Amanda L. Tidmore, 35F, Intelligence Analyst

Originally published in Military Intelligence Professional Bulletin, July – December 2025, https://www.lineofdeparture.army.mil/Journals/Military-Intelligence/About-Military-Intelligence-Professional-Bulletin/

Introduction

The U.S. Army strategic contexts of competition, crisis, and armed conflict correspond to and support the joint competition continuum. Currently, the People's Republic of China and Russia are in a constant state of competition with the United States, seeking to gain superiority through significant military, economic, and political advantages. The operational environment continues to evolve in response to these adversaries' increasing capabilities, and the Army must prepare to fight in contested environments. Therefore, the Army established multidomain operations as its operational concept. Multidomain operations encompass a combined arms approach to operations in the land, maritime, air, space, and cyberspace domains, while maneuvering across the physical, information, and human dimensions. The intelligence warfighting function is key to providing the Army with relative advantages and windows of opportunity to overcome adversary defenses. The extended operational environment poses significant challenges for the intelligence warfighting function. To meet those challenges, the Army must leverage big data and technology solutions to develop new sensing capabilities that can penetrate, survive, and collect information.

The Operational Environment

The operational environment encompasses the human, physical, and information dimensions within each domain. Collectively, the combination of domains and dimensions are analyzed and described through the operational variables: political, military, economic, social, information, infrastructure, physical, and time (PMESII-PT), applied within the context of the mission variables: mission, enemy, terrain and weather, troops and available support, time available, and civil considerations (METT-TC).[1] As the Army shifts strategic priorities from counterinsurgency operations to large-scale combat operations, the operational environment will be increasingly difficult to navigate for the intelligence warfighting function. Peer threats with capabilities across all domains will pose a significant challenge. "The PRC [People's Republic of China] has expanded and modernized nearly every aspect of the PLA [People's Liberation Army], with a focus on offsetting U.S. military advantages."[2] Knowledge of the future operational environment will be imperative to reducing operational uncertainty for fighting and winning in complex environments, and the intelligence warfighting function will play a vital role in supporting operations across all domains. Army intelligence professionals must understand each domain, leverage intelligence architecture, collaborate with other military services, and provide intelligence support to all echelons to be effective.

"In addition to expanding its conventional forces, the PLA is rapidly advancing and integrating its space, counterspace, cyber, electronic, and informational warfare capabilities to support its holistic approach to joint warfare."[3] Intelligence sets the conditions for theater operations; gaining situational understanding of the operational environment will drive success against future threats in multidomain operations and a potentially contested operational environment.

The Tactical Problem

Antiaccess (A2) and area denial (AD) are approaches adversaries use to prevent friendly forces from entering an operational area and then hinder their ability to maneuver within that area.[4] A2 and AD systems combine long-range capabilities, such as antiship, antiair, and antiballistic weapons, intended to impede movement into the operational environment, with short-range capabilities, such as electromagnetic warfare and integrated air defense systems, to decrease maneuverability once inside. Army intelligence faces a series of challenges in adapting to evolving A2 and AD environments and operating successfully in multidomain operations.

Commanders require accurate, relevant, and predictive intelligence to understand the threat across the strategic contexts of competition, crisis, and armed conflict. A2 and AD will pose unique problems for Army intelligence during armed conflict. Future Army intelligence collection systems will need to be survivable aerial platforms that can overcome A2 and AD systems and achieve stand-off through high altitudes. Today's Army intelligence, surveillance, and reconnaissance collection is susceptible to contested airspace and has limited collection ranges. Currently, corps and division intelligence lack sufficient organic assets capable of penetrating peer threat stand-off defenses to support targeting, situational understanding, and decision making. To be successful, the Army must be capable of penetrating the A2 and AD systems in regional areas that have spent the last decade building advanced weapon systems. In future armed conflict, peer adversary defenders will have an advantage because they will be defending specific A2 and AD zones that the United States will need to penetrate to be effective in follow-on operations.

The Tactical Solution

Army 2030 initiatives include significant changes that will enable divisions to be more effective by task organizing for purpose, modernizing key capabilities, and providing

future capacities at echelon to defeat peer adversaries.[5] Multidomain deep sensing, along with other information collection, will be instrumental in successfully maneuvering to defeat adversary A2 and AD capabilities. The ability to penetrate, survive, and collect information during multidomain operations will provide early warning, current intelligence, and target intelligence to inform and drive operations. Modernization efforts for collection platforms are necessary to ensure an intelligence advantage in contested environments.

The Multi-Domain Sensing System (MDSS) will provide the Army with extended endurance over wide areas, enabling it to counter A2 and AD systems. Its sensors will collect, process, correlate, and analyze using artificial intelligence (AI) and machine learning (ML) technologies. "MDSS will use quantum communication and information technology, AI, and other autonomous solutions to rapidly ingest, sort, process and archive data at speeds and measures of performance far beyond human capacity."[6] Deep sensing capabilities will provide a military advantage on the battlefield because future collection platforms will be able not only to penetrate A2 and AD systems' defenses, but also to collect at stand-off distances, providing intelligence support to multiple echelons. The Army is currently piloting the MDSS High Accuracy Detection and Exploitation System (HADES). "HADES will address Army requirements for medium to high altitude aerial ISR [intelligence, surveillance, and reconnaissance] capabilities to rapidly gain and maintain situational understanding, freedom of maneuver, information overmatch, and decision advantage in the MDO [multidomain operations]."[7] Deep sensing capabilities will be imperative to enable the Army to generate combat power for deep operations.

The Army is also adopting the Tactical Intelligence Targeting Access Node (TITAN), a system that leverages AI and ML to process sensor data, providing direct support to targeting and battlefield situational awareness during multidomain operations. TITAN will increase the speed and accuracy of intelligence collection, processing, and dissemination. HADES and TITAN both support the Department of Defense's fiscal year 2023 data, analytics, and AI adoption strategy to accelerate decision advantages over near-peer and peer threats. "The Department's investments in data, analytics, and AI will address key operational problems identified in the 2022 NDS [National Defense Strategy], fill validated gaps to enhance the warfighting capabilities of the Joint Force, and strengthen the enterprise foundation required to sustain enduring advantages."[8]

Fighting For Intelligence

The intelligence warfighting function task list is a comprehensive but incomplete listing of the Army intelligence warfighting function's responsibilities, missions, and operations. It includes providing intelligence support to force generation, providing support to situational understanding, conducting information collection, and providing intelligence support to targeting.[9] The intelligence warfighting function faces a significant challenge when attempting to provide effective and flexible intelligence during multidomain operations due to the potential contested environment across all domains. This challenge, referred to as fighting for intelligence, drives actions by the commander and staff "to identify and ultimately open windows of opportunity at the right time and place to leverage one or more capabilities across domains,"[10] leading to exploiting a relative advantage.

Integrating AI and ML technologies is necessary to collect intelligence and provide deep sensing capabilities in A2 and AD environments. Threat A2 and AD capabilities will directly impact the Army's ability to collect intelligence on threats, challenging the ability to fight for intelligence during competition, crisis, and armed conflict. MDSS will provide the Army with a tool to fight for intelligence across echelons and facilitate intelligence support to ground commanders through deep, close, and rear operations. Although multidomain operations will present numerous challenges, the intelligence warfighting function can successfully navigate these challenges if the Army capitalizes on the advantages that AI and ML technologies will bring to intelligence collection platforms.

Endpoints

[1]Department of the Army, Field Manual (FM) 5-0, *Planning and Orders Production* (Government Publishing Office [GPO], 2024), 5, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN42404-FM_5-0-000-WEB-1.pdf.

[2]Department of Defense, *2022 National Defense Strategy of the United States of America* (GPO, 2022), 4, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

[3]Ibid., 4.

[4]Department of the Army, FM 3-0, *Operations* (GPO, 2025), 33.f

[5]John Dolan et. al, "Enabling the Division in 2030: Evolving Division Reconnaissance and Security Capabilities," *Armor CXXXVV*, no. 2 (Spring 2023): 13-17, https://www.benning.army.mil/Armor/eArmor/content/issues/2023/Spring/2Dolan_Pelham_Sickler_Speakes_Frederick23.pdf.

[6]Army Futures Command (AFC), AFC Pamphlet 71-20-3, *Army Futures Command Concept for Intelligence 2028* (AFC Futures and Concept Center, 2020), 70, https://api.army.mil/e2/c/downloads/2021/01/05/26b729a6/20200918-afcpam-71-20-3-intelligence-concept-final.pdf.

[7]Daniel Baldwin, "The Future of Army Deep Sensing," News, U.S. Army website, January 19, 2024, https://www.army.mil/article/273077.

[8]Department of Defense, *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage* (GPO, 2023), 5, https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

[9]Department of the Army, FM 2-0, *Intelligence* (GPO, 2023), B-1.

[10]Ibid., 1-28.

References:

The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines. Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

Feickert, Andrew. *The Army's AimPoint and Army 2030 Force Structure Initiatives*. Congressional Research Service, 2022. https://crsreports.congress.gov/product/pdf/IF/IF11542.

Intelligence Community Assessment: Annual Threat Assessment. Office of the Director of National Intelligence, 2024. https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annualthreat-assessment-of-the-u-s-intelligence-community.

Mazarr, Michael J. *Understanding Competition: Great Power Rivalry in a Changing International Order–Concepts and Theories*. Rand Corporation, 2022. https://www.rand.org/pubs/perspectives/PEA1404-1.html.

National Military Strategy 2022. Office of the Chairman of the Joint Chiefs of Staff, 2022. https://www.jcs.mil/Portals/36/NMS%202022%20_%20Signed.pdf.

Sayler, Kelley M. *Artificial Intelligence and National Security*. Congressional Research Service, 2020. https://www.congress.gov/crs-product/R45178.

Know Thy Enemy: Using AI to Create Enemy Commanders

By Cmdr. Stephen P. Ferris, U.S. Navy (Retired) and CPT Raymond M. Ferris, U.S. Army

From Military Intelligence Professional Bulletin, July – December 2025, https://www.lineofdeparture.army.mil/Journals/Military-Intelligence/About-Military-Intelligence-Professional-Bulletin/

Introducing the Digital Enemy Commander

MILITARY INTELLIGENCE faces unprecedented challenges in understanding adversary behavior in this current era of multi-domain warfare. One promising way forward is the use of artificial intelligence (AI), which is rapidly becoming the most transformative technology in military operations since the advent of digital communications, offering unprecedented capabilities to understand enemy intent and predict their behaviors. AI fundamentally reshapes how intelligence officers analyze threats, predict enemy actions, and support their commanders' decision-making. This essay explores a new application of AI for the intelligence officer: the development of an AI persona who can serve as the digital enemy commander or red team. This digital commander can reflect the tactics, strategies, and mindset of the opposing force, allowing intelligence professionals an unprecedented insight into adversary intentions and decisions.

Traditional intelligence analysis faces significant limitations that constrain its effectiveness. Human analysts, despite their expertise and intuition, struggle with inherent cognitive biases which can skew threat assessments and operational recommendations.[1] The information processing capacity of humans becomes increasingly insufficient when confronted with an abundance of data from satellite imagery, signals intelligence, human sources, and open-source materials.[2] Most critically, traditional intelligence methods fail to identify the decision-making patterns of adversaries who operate from fundamentally different cultural, ideological, or strategic frameworks.[3]

The creation of an AI agent who mimics the thinking of an adversary is a significant technological advancement, offering intelligence officers a valuable tool to anticipate enemy behaviors. These sophisticated AI agents can function as digital enemy force commanders, trained on comprehensive datasets of adversary behavior, doctrine, communications, and decision-making patterns. Unlike traditional analysis that simply examines previous enemy actions, these AI agents enable intelligence officers to anticipate the enemy, providing real-time insights into how adversary commanders might respond to dynamic battlefield conditions, strategic pressures, or friendly force actions.

This concept already exists in the private sector with companies employing AI executives or managers to model competitor decision-making processes or regulatory decision making.[4] Companies leverage sophisticated AI systems to analyze executive communication patterns, strategic announcements, and market responses to predict competitor responses. These business applications show the ability of AI to discover complex human decision-making patterns and predict future actions based on historical data.

The integration of an AI-developed digital commander with current intelligence doctrine and best practices represents an evolutionary leap forward in the practice of military intelligence. These AI systems complement existing doctrinal frameworks by providing dynamic, data-driven insights that augment human analytical judgment. For the intelligence officer, these adversarial agents offer the ability to conduct virtual consultations with the enemy commander and receive an immediate enemy response to a proposed course of action, complete with military reasoning.

Using AI agents to simulate the decision-making of an enemy commander offers substantial benefits. The AI agent's ability to model specific adversarial thought processes, command preferences, and tactical doctrines results in enhanced predictive accuracy. These digital commanders reflect likely enemy responses to friendly force movements by using the cognitive frameworks and strategic priorities of actual opposing leaders. Another benefit is reduced analytical bias: the AI agent has the capacity to think from the adversary's perspective without the constraints of friendly force cultural or doctrinal assumptions. Real-time adaptive modeling allows these digital enemy commanders to evolve their decision-making as new intelligence is collected. This ability to adapt provides intelligence officers with dynamic threat assessments that reflect how adversary commanders might respond to developing situations. Strategic planning also improves through the AI agent's ability to role-play enemy decision-making across multiple military scenarios, resource allocations, and political developments.

Digital Adversaries and Intelligence Doctrine

Current intelligence doctrine emphasizes the analysis of adversary capabilities, intentions, and operational methods through intelligence preparation of the operational environment (IPOE).[5] This analysis of the adversary centers on understanding enemy force structures, operational patterns, decision-making hierarchies, and adaptive capabilities. IPOE focuses on historical precedent analysis, war gaming simulations, cultural and behavioral profiling of enemy leadership, war gaming simulations, and red team exercises. The U.S. military's red team tradition began with the Army War College's use of opposing forces in the early 1900s, evolved through World War II's strategic

war gaming, and was refined during Cold War exercises like REFORGER and ABLE ARCHER.[6] These exercises employed human analysts and military personnel to think and act like enemy commanders. They attempted to replicate adversary decision-making processes, tactical preferences, and strategic posturing. The National Training Center at Fort Irwin institutionalized this approach through the Opposition Forces (OPFOR) program, where American units trained against forces employing Soviet tactics and equipment.

Red force exercises consistently show that human role-players, despite their expertise, face limitations in maintaining adversary perspectives over extended periods. Cultural biases, fatigue, and unconscious adoption of friendly force thinking compromise red team effectiveness.[7] Human cognitive limitations become apparent when processing large datasets from multiple intelligence sources. Time constraints during crisis situations often force analysts to rely on incomplete assessments.

AI adversary agents represent the natural evolution of the use of red force thinking in intelligence assessment. They consistently simulate the enemy's perspective through continuous learning, bias-free analysis, and unlimited processing capacity. AI adversary agents do not suffer the limitations of human red force commanders.

Intelligence doctrine recognizes that military intelligence personnel must continuously adapt their analytical approaches to anticipate adversary actions. Doctrine acknowledges that potential enemies represent sophisticated, thinking opponents with significant capabilities and resources. The existence of these adversaries who creatively respond to our actions necessitates a digital agent to model enemy behaviors in real time.[8]

AI opportunities within existing doctrine focus on areas where human-AI collaboration can enhance analytical capabilities rather than replace human insight. Digital enemy commanders can complement current practices by providing continuous behavioral modeling that updates in real time and processes multi-source intelligence beyond human capacity. They can also identify subtle correlations across vast datasets and generate multiple scenario predictions for strategic planning purposes. Doctrine compatibility ensures that AI agents support rather than supplant human intelligence analysts. The human element remains critical in final decision-making while AI enhances both the quality and speed of information processing.

Technical Foundation and Implementation

Digital enemy commanders represent a specialized application of AI designed to replicate specific enemy decision-making processes and strategic thinking patterns through sophisticated behavioral modeling techniques. These techniques integrate multiple AI technologies such as machine learning algorithms for behavioral pattern recognition, natural language processing for communication analysis, game theory models for strategic decision simulation, and reinforcement learning mechanisms for adaptive behavior modification.

The foundation for AI adversary modeling draws heavily from successful business intelligence applications where AI systems analyze senior executives' behaviors and competitive strategies. The Strategic Consortium of Intelligence Professionals (SCIP), the world's largest global intelligence association with over 15,000 members in 120 countries, emphasizes the growing importance of data-driven competitive intelligence in understanding executive decision-making patterns.[9] Business intelligence practices use AI to model competitor behavior by analyzing communication patterns, press releases, strategic announcements, financial decisions, and operational changes.

Business applications reveal several key insights applicable to military adversary modeling.[10] AI systems excel at identifying subtle patterns in executive communication that human analysts might miss, such as linguistic markers indicating strategic shifts or decision-making stress. Machine learning algorithms can correlate seemingly unrelated data points such as economic indicators, personnel changes, market pressures, and public statements to predict changes in corporate marketing or operational directions. Natural language processing analyzes leadership rhetoric for signals of policy shifts, risk appetite, and strategic priorities.

Training an AI agent to act like an enemy commander requires the collection and analysis of diverse data sources that reveal adversary decision-making patterns. Historical military operations provide foundational training data, including documented enemy tactical decisions, strategic choices, and operational adaptations across various conflict scenarios. Leadership communications, including speeches, military directives, doctrine publications, and strategic guidance documents, indicate cognitive frameworks and operational philosophies. Cultural and ideological materials, such as military education curricula, historical texts, and philosophical or political works that influence enemy thinking, provide essential context for understanding an adversary's worldview.

Intelligence databases containing years of enemy practices, response timelines, and adaptation strategies offer quantitative foundations for behavioral modeling. Economic and political decision-making records show how external pressures influence military choices. Communication patterns reveal leadership interaction styles, decision-making hierarchies, and information flow preferences. Exercise and training records from enemy forces imply preferred tactics, operational concepts, and adaptation capabilities.

Real-time data processing mechanisms employ distributed computing architectures that can scale with intelligence volume and complexity. Historical database integration provides contextual depth by incorporating decades of adversary behavior patterns, enabling digital agents to identify long-term trends and cyclical patterns in enemy decision-making easily overlooked by human observers. Social media and opensource intelligence adds contemporary behavioral indicators that complement traditional intelligence sources.

The computational foundation of digital adversary systems relies on sophisticated decision-making algorithms that enable complex behavioral modeling.[11] Bayesian networks manage uncertainty and probability distributions across multiple scenario possibilities. Neural networks provide complex pattern recognition capabilities for identifying subtle behavioral correlations. Decision trees model tactical choice

hierarchies based on adversary doctrine and historical preferences. Monte Carlo simulations generate outcome probability assessments for strategic planning support.

Decision-Making Algorithms Defined

Bayesian Network: A type of graphical model representing probabilistic relationships among a set of variables. A Bayesian network is a visual map of cause-and-effect relationships that assist in making informed predictions.

Neural Network: Unlike Bayesian networks which rely on predefined relationships, neural networks, which are modeled on the human brain, learn relationships directly from raw data. These networks employ interconnected nodes organized into three layers: the input layer receives data; the hidden layer (i.e, the "brains" of the network) processes that data; and the output layer generates a prediction or conclusion.

Decision Tree: One of the most intuitive tools in machine learning, a decision tree is essentially a flowchart using a series of if-then-else rules to predict an outcome. At its simplest, a decision tree breaks complex problems down into smaller, more easily manageable decisions and produces a visual representation of the possible outcomes of each choice.

Monte Carlo simulation: These simulations use probability distributions to solve complex problems by using randomness and repetition to explore many possible outcomes—effectively predicting the future by running "what if" scenarios thousands (or millions) of times to estimate the likelihood of different results.

Behavioral modeling for creating a digital adversary focuses on three primary dimensions: cognitive architecture replication, cultural framework integration, and strategic preference modeling.[12] Cognitive architecture replication involves mapping individual adversary leaders' decision-making patterns, risk tolerance levels, and cognitive biases. For example, an AI agent might incorporate a specific commander's documented preference for aggressive flanking maneuvers and willingness to accept high casualty rates, thus predicting bold tactical choices over defensive consolidation. Cultural framework integration incorporates social, economic, and political environmental factors that influence adversary behavior. A system modeling a clan-based society leader, for example, would include face-saving requirements, religious calendar constraints, and tribal balance considerations when predicting military decisions. Strategic preference modeling analyzes historical decision patterns to predict future choices under similar circumstances. As an example, an enemy commander who historically reinforces failing positions rather than withdrawing would likely repeat this pattern, allowing the digital adversary to predict the commitment of reserves rather than tactical repositioning.

Applications Across the Threat Spectrum

Digital adversaries demonstrate their versatility across the entire threat spectrum, from immediate tactical challenges to long-term strategic competition. These AI-powered agents adapt their modeling approaches to match the scope and complexity of different operational environments. This section describes how adversary simulation capabilities scale from battlefield-level decision support to national-level strategic planning.

- *Tactical intelligence support* provides immediate operational value through battlefield prediction and counter-strategy development. Unit deployment and movement pattern analysis provided by the digital enemy commander can identify enemy tactical preferences and likely courses of action. Identification of communications and logistics vulnerability reveals weak points in adversary operational systems. Real-time tactical recommendations provide commanders with response options based on evolving battlefield conditions.
- *Crisis response and conflict escalation* scenarios benefit significantly from the modeling of enemy intent. Deescalation strategy development involves predicting adversary responses to various diplomatic and military initiatives. For instance, it might model how a regional power responds to graduated economic sanctions versus immediate military action. Red line identification and boundary testing scenarios help commanders understand adversary tolerance levels and likely escalation triggers. Negotiation strategy optimization provides insights into adversary priorities and acceptable compromise positions. Unintended consequence prediction and mitigation identify potential second and third-order effects of proposed actions, such as anticipating how arms sales to regional allies might trigger adversary military modernization programs or shift alliance structures.
- *Training and exercise applications* of digital adversaries enhance military preparedness through more realistic adversary simulation. Enhanced red team capabilities provide more sophisticated opposition forces for deployment in military exercises. Realistic adversary behavior simulation creates training scenarios that better prepare personnel for actual combat conditions. Digital enemy commanders can stress the decision-making of friendly forces and create highly challenging scenarios.
- *Counterintelligence operations* gain significant capability with the deployment of a digital enemy commander. This digital enemy acts as a virtual opponent, continuously challenging friendly counterintelligence assessments by simulating hostile intelligence intent and incorporating multi-domain threats. The digital adversary models enemy intelligence collection practices, such as predicting embassy personnel positioning or anticipating coordinated social media strategies. Through adversarial simulation, this digital enemy reveals potential deception campaigns by offering alternative narratives and cross-platform coordination that mirrors actual foreign intelligence behaviors. The virtual opponent validates double agent operations and source

reliability by adopting the adversary's perspective to identify operational vulnerabilities and asset compromise indicators. Most critically, the digital enemy commander actively models adversary influence on operational timelines and predicts enemy responses to friendly countermeasures.

- *Strategic intelligence* can incorporate sophisticated digital agents to serve as force multipliers in adversary analysis and long-term planning. By analyzing resource allocation patterns, technology acquisition strategies, and force modernization priorities, digital agents can anticipate how adversaries will evolve militarily over time. This analysis extends beyond hardware to encompass policy and doctrine evolution, forecasting how an adversary's strategic posture might respond to geo-political and military developments.
- *Examining alliance structures and partnership network*s is key to understanding adversary behavior. The digital enemy can describe how adversary coalitions respond to strategic pressures and opportunities, revealing the web of relationships that shape collective decision-making. These agents can explain alliance politics, economic interdependencies, and shared strategic interests that influence how adversary blocs coordinate their responses to external challenges.

The sophistication of these digital agents becomes evident when assessing how economic and political decisions cascade into military action. Digital adversaries can predict the effects of economic sanctions, political transitions, or diplomatic pressure on enemy military actions or likely countermoves. This capability also allows intelligence officers to anticipate second- and third-order effects before a decision is actually executed, enabling more informed strategic planning.

Mitigation Strategies for Implementation Challenges

Technical limitations present various challenges to adopting adversary digital agents in intelligence operations.[13] Data quality significantly limits AI system accuracy, particularly when historical data is incomplete, fragmented, or unreliable. Computational resource requirements for sophisticated behavioral modeling and prediction can quickly exceed available processing capacity. This is especially true when modeling complex, adaptive adversary networks. Further, model bias and accuracy concerns become critical when training datasets inadequately capture the full spectrum of variability in adversary behavior, tactics, and decision-making processes.

Adversary adaptation and countermeasures pose continual problems to the usefulness of digital adversary effectiveness. Enemies engaged in evasive attacks could attempt to deceive AI systems by developing new types of digital camouflage.[14] Sophisticated adversaries might deliberately alter their behavior patterns to confuse AI agents. Deception campaigns specifically designed to exploit AI vulnerabilities could compromise the accuracy of digital agents. Counter-AI technologies can enable adversaries to identify and neutralize friendly AI capabilities.

Operational challenges can create barriers that complicate the use of digital adversary agents across intelligence organizations. Over-reliance on AI recommendations risks degrading human analytical skills and intuition, potentially creating dangerous dependencies that erode the critical thinking capabilities of human analysts. This concern is compounded by the problem of integration with legacy intelligence systems, which requires new technical resources, specialized expertise, and extensive system modifications. Experienced analysts' resistance to training and adoption can slow implementation even further, as seasoned professionals often cite their own field experience in questioning the usefulness of AI-generated insights. Meanwhile, digital adversaries' real-time processing demands place enormous stress on the existing computing infrastructure, creating bottlenecks that can compromise operational effectiveness during critical intelligence gathering periods.

Human oversight also becomes increasingly difficult when AI agents rely on thousands of data points to draw conclusions, making it nearly impossible for human analysts to verify AI output accuracy.[15] The growing complexity of modern AI systems frequently exceeds human comprehension capabilities, creating significant accountability gaps in intelligence assessment processes. Successful integration, therefore, requires careful consideration of the existing analyst workflow while maintaining human judgment as the ultimate decision-making authority. This ensures that AI enhances rather than replaces human expertise in critical intelligence operations.

Effective mitigation strategies can successfully integrate digital adversary agents into intelligence operations as valuable tools for assessing enemy intentions and likely courses of action.[16] Technical challenges require targeted solutions that ensure system reliability and accuracy. Robust data validation protocols address incomplete historical intelligence by establishing quality thresholds and cross-referencing multiple sources. Classification safeguards prevent inadvertent disclosure by implementing automated security checks and human review processes. Scalable computing architectures accommodate sophisticated behavioral modeling without overwhelming existing infrastructure. Diverse training datasets capture the full spectrum of adversary behavior patterns across operational contexts and geographical regions.

Operational integration demands careful attention to analyst workload and organizational culture. Structured training programs help analysts understand system capabilities and limitations while building confidence in appropriate tool usage. Human-AI collaboration protocols can position digital adversary agents as tools for analytical support rather than decision-making replacements. Experienced analysts maintain primary authority over intelligence assessments while leveraging enhanced processing capabilities for complex pattern recognition. Gradual implementation phases further allow organizations to adapt to this new method of intelligence analysis.

Continuous improvement processes also ensure the long-term effectiveness of digital agents. Regular system updates address evolving adversary tactics and emerging threat patterns. Performance monitoring identifies

degradation or potential countermeasures before they impact operations. Feedback mechanisms capture analyst insights to refine system accuracy and usability.

Conclusion

AI is fundamentally transforming how intelligence officers understand, analyze, and predict adversary behavior. This essay focuses on how AI can be used to create digital enemy commanders, providing unprecedented insight into enemy intentions and behaviors. Creation of digital adversary agents represents more than technological advancement; it constitutes a major shift in military intelligence methodology that allows intelligence officers to understand and predict the behavior of enemy commanders.

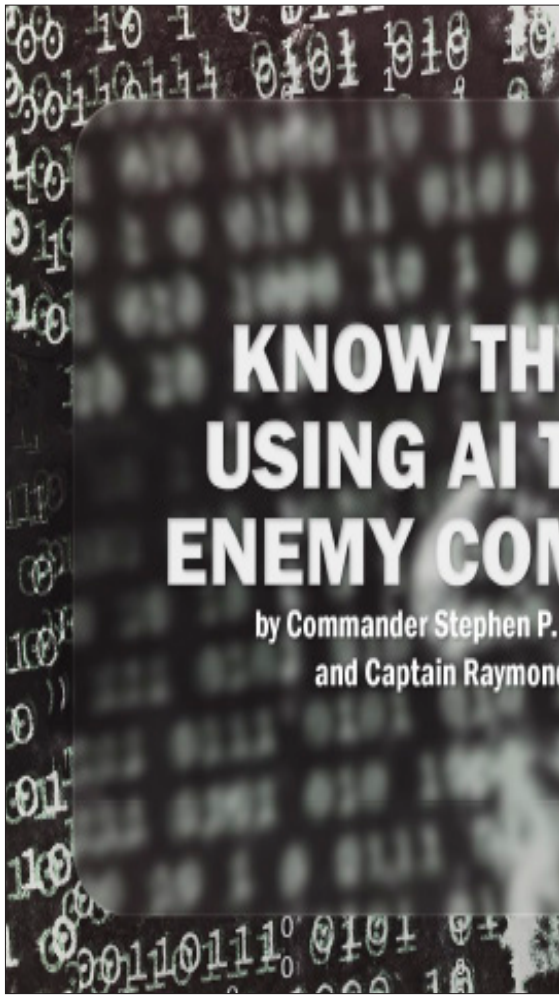
The development of digital adversary agents offers intelligence officers the capability to engage in virtual consultations with enemy commanders, testing proposed courses of action and receiving immediate adversary responses. This use of AI enables intelligence professionals to surpass traditional analytical limitations through literal adoption of adversary leaders' mindsets. The intelligence officer gains access to enemy thinking patterns, decision-making processes, and strategic preferences that can be used in real-time.

The implications of digital adversaries extend beyond the immediate tactical advantages they provide to intelligence officers. Intelligence officers supported by a digital enemy commander gain the capability to continuously analyze enemy behavior, predict adversary responses to friendly actions, and identify strategic vulnerabilities often missed by traditional analysis. Digital adversaries allow friendly forces to respond much faster to enemy actions, anticipate enemy intentions more accurately, and develop more effective strategic planning across all levels of military operations.

The datasets required to develop a digital agent are comprehensive enough to ensure a high degree of reliability for the recommendations that they generate. As they learn through continuous exposure to new intelligence inputs and validation against actual enemy behavior, these digital agents become increasingly sophisticated representations of adversary command thinking.

For the modern intelligence officer, digital adversary agents represent an indispensable tool for achieving analytical superiority in the global security environment. As adversaries like China advance their own military AI capabilities, the United States and its allies must leverage these technologies to preserve their intelligence advantages. The integration of digital agents with intelligence doctrine provides a foundation for revolutionary improvements in understanding and countering enemy threats.

The future of military intelligence lies in the integration of human expertise with AI capabilities. [17] The intelligence officer is the interface between the insights of the digital adversary and command decision-making. Digital enemy commanders will become essential tools in the intelligence officer's tool set. They will provide new capabilities to anticipate an adversary's thinking and to predict enemy actions at a level of accuracy impossible with traditional intelligence analysis. This transformation positions military intelligence at the forefront of the technological innovations that will shape the future of 21st century warfare.



Endpoints

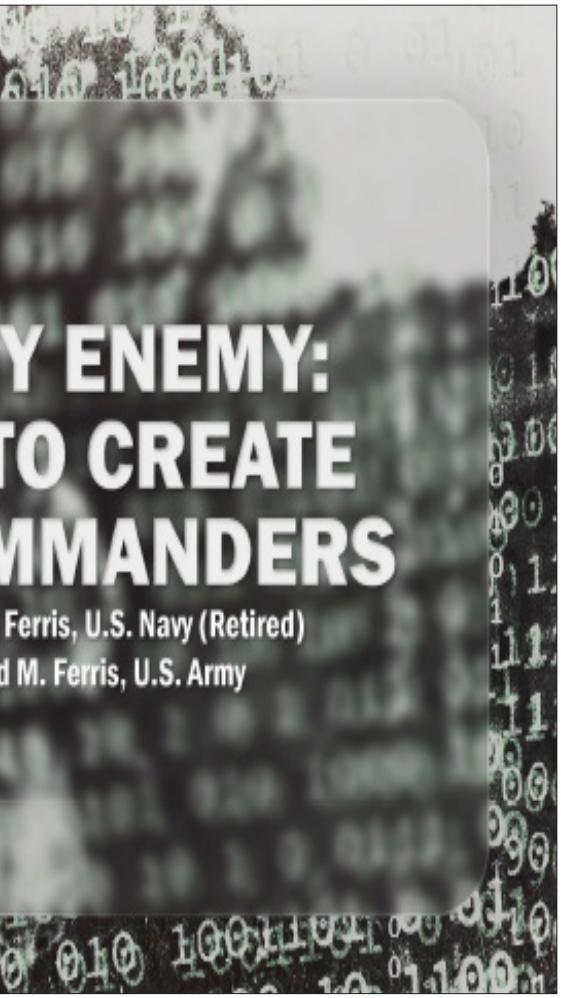
[1]Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (27 September 1974), 1124-1131, https://www.science.org/doi/10.1126/science.185.4157.1124. Human decision-making is systematically influenced by numerous cognitive biases that can lead to errors in judgment and analysis. Kahneman and Tversky's foundational research identified key heuristics including confirmation bias (seeking or giving undue weight to information that confirms existing beliefs), availability heuristic (overweighting easily recalled information), and representativeness heuristic (judging probability by similarity to mental prototypes); Daniel Kahneman, *Thinking, fast and slow* (Farrar, Straus and Giroux, 02 April 2013). Additional biases include anchoring (over-relying on first information), overconfidence in one's abilities, loss aversion, and framing effects, which Kahneman later synthesized in his comprehensive analysis of dual-process thinking; Thomas Gilovich, Dale Griffin, and Daniel Kahneman, eds., Heuristics and Biases: The Psychology of Intuitive Judgment (Cambridge University Press, 08 July 2022). These systematic deviations from rational decision-making models demonstrate how intuitive judgment often leads to predictable errors.

[2]Herbert A. Simon, "A behavioral model of rational choice," *The Quarterly Journal of Economics* 69, no. 1 (February 1955), 99-118, https://doi.org/10.2307/1884852. Human cognitive processing is constrained by limited attention, memory, and computational capacity, leading to systematic biases and heuristic-based decision-making rather than optimal choices.

[3]David Robson, "How East and West think in profoundly different ways," *BBC*, 19 January 2017, https://www.bbc.com/future/article/20170118-how-east-and-west-think-in-profoundly-different-ways.

[4]Pratik Kothari and Stephen P. Ferris, "Strategic Generosity: The Business of Political Contributions," *Social Science Research Network Electronic Journal* (28 April 2025), https://dx.doi.org/10.2139/ssrn.5241811. The authors use a sample of 4,949 digital corporate executives and find that executives primarily view political contributions as strategic investments that extract economic value and secure critical information to navigate policy landscapes.

[5]Headquarters Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Government Publishing Office, 01 October 2023). IPOE is defined here as "the systematic process of analyzing the mission variables of enemy, terrain, weather and civil



considerations in an area of interest to determine their effect on operations." The name change from "intelligence preparation of the battlefield" to "intelligence preparation of the operational environment" better reflects the multidomain nature of the operational environment.

[6]David Alan Rosenberg, "Being 'Red:' The Challenge of Taking the Soviet Side in War Games at the Naval War College," *Naval War College Review* 41, no. 1 (Winter 1988): 81-93, https://digital-commons.usnwc.edu/nwc-review/vol41/iss1/7/; Micah Zenko, *Red Team: How to Succeed By Thinking Like the Enemy* (Basic Books, 2015).

[7]Headquarters Department of the Army, *The Red Teaming Handbook*, 9th ed. (U.S. Army, 2024, distribution limited).

[8]FM 2-0, *Intelligence*, 1-1—2-35.

[9]"Strategic Consortium of Intelligence Professionals (SCIP)," SCIP, https://www.scip.org/. Originally called the Society of Competitive Intelligence Professionals, SCIP was founded in 1986 to promote competitive, market, and strategic intelligence practices in enterprise, academia, and government. This nonprofit organization provides education, certification programs, networking opportunities, and best practices for legal and ethical business intelligence collection and analysis, serving as the premier advocate for intelligence-driven decision-making.

[10]Pratik Kothari and Stephen P. Ferris, "Personality-Driven Procurement: AI Executives and Strategies for Federal Contracting" (Working Paper, University of North Texas, 2025). While Kothari and Farris (2025) focus on strategies followed by CEOs to gain advantages in the federal contracting process, in this paper the authors survey a sample of digital CEOs to understand the reasons for corporate donations to political candidates.

[11]Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach, 4th ed. (Pearson, 08 May 2020).

[12]Iuliia Kotseruba and John K. Tsotsos, "40 Years of Cognitive Architectures: Core Cognitive Abilities and Practical Applications," *Artificial Intelligence Review* 53, no. 1 (2020), 17-94, https://psycnet.apa.org/doi/10.1007/s10462-018-9646-y; Aaron J. Barnes, YuanYuan Zhang, and Ana Valenzuela, "AI and Culture: Culturally Dependent Responses to AI Systems," *Current Opinion in Psychology 58* (August 2024), https://doi.org/10.1016/j.copsyc.2024.101838.

[13]Adib Bin Rashid, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, and Mehedy Hassan Bappy, "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges," International Journal of Intelligent Systems 2023, no.1 (2023), http://dx.doi.org/10.1155/2023/8676366.

[14]Digital camouflage involves masking authentic signals, communications patterns, and behavioral signatures to deceive adversary AI systems and digital personas. Techniques include spoofing metadata, generating synthetic noise, mimicking benign traffic patterns, and creating false digital footprints that obscure genuine operational activities from automated detection and analysis algorithms.

[15]Yavar Bathaee, "The Artificial Intelligence Black Box and the Failure of Intent and Causation," *Harvard Journal of Law & Technology* 31, no. 2 (Spring 2018), 889-938, https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf.

[16]Anthony King, "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence," *Journal of Global Security Studies* 9, no. 2 (June 2024), https://doi.org/10.1093/jogss/ogae009.

[17]Michael Mayer, "Trusting Machine Intelligence: Artificial Intelligence and Human-Autonomy Teaming in Military Operations," *Defense & Security Analysis* 39, no. 4 (2023), 521-538, https://doi.org/10.1080/14751798.2023.2264070.

Operationalizing Intelligence Through Small Unmanned Aircraft Systems

By CPT Jose A. Lopez

Originally published in Military Intelligence Professional Bulletin, July – December 2025, https://www.lineofdeparture.army.mil/Journals/Military-Intelligence/About-Military-Intelligence-Professional-Bulletin/

Silent Wings Over Donetsk Ridge

Author's note: This vignette is a fictitious representation of a nonexistent unit.

THE FRIGID WINDS swept across the Donetsk Ridge as the first light of dawn struggled to pierce the overcast skies. Snow-covered hills and dense forests flanked the valley, masking the movements of both Russian and Ukrainian forces. Kaptain Oksana Marchenko, intelligence officer for Ukraine's 123rd Mechanized Brigade, stood in the tactical operations center at Kramatorsk, her brow furrowed as she analyzed the fragmented intelligence reports coming from forward positions.

The brigade's mission was to advance along the ridge toward the transport hub at Bakhmut, a vital supply line for ongoing defensive operations to the east. Success depended on precise coordination, reliable intelligence, and the ability to outmaneuver the Russian forces entrenched in the area. However, the enemy's activity was subtle but ominous. Intermittent artillery fire and sightings of loitering munitions suggested a coordinated Russian presence. The valley's jagged terrain, narrow routes, and frequent electromagnetic interference rendered traditional reconnaissance assets almost useless.

The brigade's imported small unmanned aircraft systems were limited by range and increasingly affected by Russian electronic warfare systems. The cavalry reconnaissance unit, maneuvering along icy trails, had limited visibility and feared ambushes. Their approach was deliberate and in line with the brigade's sectored collection plan, assigning areas of responsibility to each organization in an effort to synchronize collection and maximize visibility of the enemy.

The Russian response came swiftly. As two companies from the 1st Mechanized Battalion pushed through a bottleneck near Chasiv Yar, a carefully orchestrated ambush unfolded. Lancet loitering munitions struck the lead vehicles, sowing confusion. Concealed infantry and anti-tank guided missile teams launched a second wave of strikes. With visibility low and communication disrupted by jamming, the forward units were pinned down, unable to advance or retreat.

At the tactical operations center, Marchenko realized the adversary was exploiting the brigade's intelligence gaps, leveraging terrain and electronic warfare. Without real-time situational awareness, the brigade risked losing tempo and its ability to counterattack. The limits of traditional intelligence, surveillance, and reconnaissance platforms were evident, and immediate action was needed to avoid catastrophe.

U.S. Army Soldiers assigned to 1st Battalion, 4th Infantry Regiment, Joint Multinational Readiness Center, Hohenfels, Germany, remotely operate a quadcopter in the Hohenfels Training Area, during Combined Resolve X, May 2, 2018. (U.S. Army photo by 1LT Matt Blubaugh)

Maximizing Capabilities

The fictional scenario of Kaptain Marchenko's struggle in Donetsk illustrates a critical challenge modern militaries face: the integration and synchronization of small unmanned aircraft systems (SUAS) within combat operations. This article seeks to drive a necessary discussion of the critical role of SUAS in enhancing situational awareness, target acquisition, and decision making at the brigade level. The introduction of SUAS revolutionized traditional reconnaissance methods and continues to empower commanders to shape the battlefield, enabling greater agility and precision in dynamic environments. This article presents two key frameworks—the Sector Collection Approach and the Ready Reserve Concept—to optimize SUAS employment and emphasizes the importance of integrating collection management into operational planning. These processes align with the Army's Transformation in Contact effort, where the collection manager must evolve from an asset allocator to an advisor on effects and capabilities.

Recent military conflicts illustrate the consequences of desynchronized intelligence, surveillance, and reconnaissance (ISR) collection. Uncoordinated and ill-equipped collection efforts create intelligence gaps, often leading maneuver forces to advance blindly into well-prepared enemy defenses. The U.S. Army is currently fielding short-, mid-, and long-range reconnaissance capabilities (particularly SUAS) at the brigade level that present a new set of opportunities and challenges. Without a standardized framework for integrating SUAS, intelligence professionals struggle to effectively drive operations and targeting. The war in Ukraine provides a clear demonstration of this challenge, with units facing ambushes and tactical setbacks due to inadequate real-time intelligence.[1] These lessons underscore the urgent need for brigades to evolve their ISR collection practices. By leveraging SUAS capabilities, units can maintain continuous surveillance, enable timely targeting decisions, and reduce operational vulnerabilities. Adapting ISR methodologies at the brigade level is crucial to preventing tactical paralysis and maintaining a decisive edge on the modern battlefield.[2]

To fully leverage SUAS capabilities, commanders must fundamentally shift their perspective on reconnaissance. Instead of viewing it as a set of discrete tasks, they need to embrace reconnaissance as an interconnected system.[3] This paradigm shift treats SUAS as expendable assets, prioritizing intelligence gathering over platform preservation and accepting calculated losses to ensure mission success. This allocation of assets and the acceptance of potential losses will always be a commander-dependent decision based on the overall maneuver.[4] By adopting this mindset, brigade-level leaders can maximize their collection assets, ensuring timely, reliable intelligence that drives decision making. This approach mitigates reactive information gaps and fully harnesses the transformative potential of SUAS in modern warfare.

Maximizing the use of SUAS fundamentally transforms reconnaissance and intelligence operations by reducing risk, extending operational reach, and shaping the battlespace.[5] A U.S. Army brigade with short-, mid-, and long-range reconnaissance SUAS can simulate activity, deceive adversaries, and gather intelligence in real time, rather than relying solely on physical troop movements to provoke enemy reactions. For example, SUAS equipped with electronic warfare payloads could potentially disrupt enemy air defense radars, a capability previously limited to higher-echelon assets. Such capabilities conceal true operational intent and manipulate adversary perceptions, shaping their decision making before direct engagement.[6]

Theoretical Frameworks for Employment

The modern battlefield demands rapid intelligence collection, analysis, and action for operational success. The Joint Multinational Readiness Center is uniquely postured to observe diverse collection practices across light, medium, and heavy U.S. units undergoing transformation in contact, as well as multinational brigades, and, most importantly, through dialogue with Ukrainian soldiers being trained as part of the Joint Multinational Training Group-Ukraine mission. Emerging tactics, techniques, and procedures identified through training with the Ukrainians showcase innovative SUAS employment and enhance brigade-level intelligence operations, particularly through the Sector Collection Approach and the Ready Reserve Concept.

The Sector Collection Approach. This approach divides the area of operations into smaller sectors aligned with named areas of interest and target areas of interest.[7] This division prioritizes collection efforts, mitigates SUAS capability gaps (terrain and limitations), and enhances control and coverage. Together with the centralized intelligence collection synchronization matrix, this approach empowers subordinate commanders to allocate SUAS within their sectors based on specific threats while maintaining the brigade's overall collection priorities. The brigade sections the area of operations and assigns requirements to its battalions, while battalions operate within these sectors, dynamically allocating and re-tasking the SUAS based on real-time threat activity and environmental factors. This structure enables early threat detection, supports the cueing of fires and maneuver forces, and creates redundancy in SUAS collection across the brigade front. By integrating doctrinal planning tools with responsive drone employment, units establish a layered SUAS network capable of adapting to complex and evolving threats.

For example, as part of a brigade defense (see figure 1), the intelligence section divides the area of operations into battalion sectors, and then further subdivides each sector into smaller collection sectors (e.g., Sector Red, Sector White, Sector Blue). Each battalion is assigned named areas of interest within its sector based on likely enemy avenues of approach.

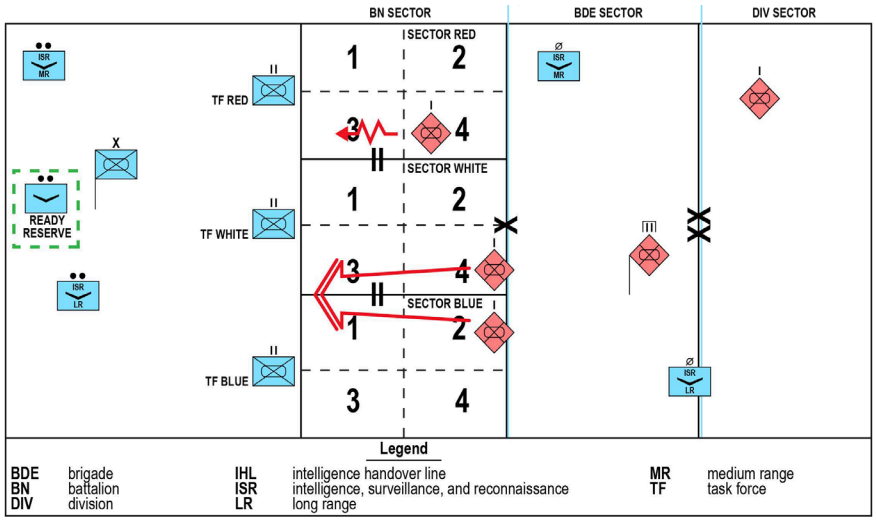


Figure 1. Sector Collection Approach

In Sector Blue, Task Force Blue observes enemy mechanized infantry elements probing near Sector Blue 1. A battalion's organic SUAS detects the movement and initiates surveillance. Minutes later, more enemy forces appear in Sector Blue 2, forming what appears to be a flanking maneuver. The battalion assigns another drone to maintain custody of the second element while cueing the brigade's mid-range reconnaissance assets forward into the brigade sector to look for follow-on forces. This also allows the long-range SUAS to continue with the developed collection plan to further confirm or deny enemy actions. These actions prevent enemy deception or a multi-pronged breach. Task Force White repositions its drones to cover adjacent sectors, enabling cross-cueing between battalions.

Because each battalion controls its ISR assets within clearly defined sectors, and brigades retain flexible ISR options, the unit reacts in real time to a complex enemy movement, reallocates sensors dynamically, and denies the adversary freedom of action.

The Ready Reserve Concept. Supporting this framework is a tactical drone reserve composed of SUAS capable of multiple effects (collect, decoy, jam, one-way attack, etc.) that offer the brigade commander operational flexibility. The Ready Reserve responds rapidly to threats or fleeting opportunities while enabling intelligence collection to develop the operational environment. The Ready Reserve's intent is to provide a flexible framework that supports operational needs, targeting, and intelligence collection, thus creating a layered intelligence network that enhances situational awareness and operational agility. (See figure 2)

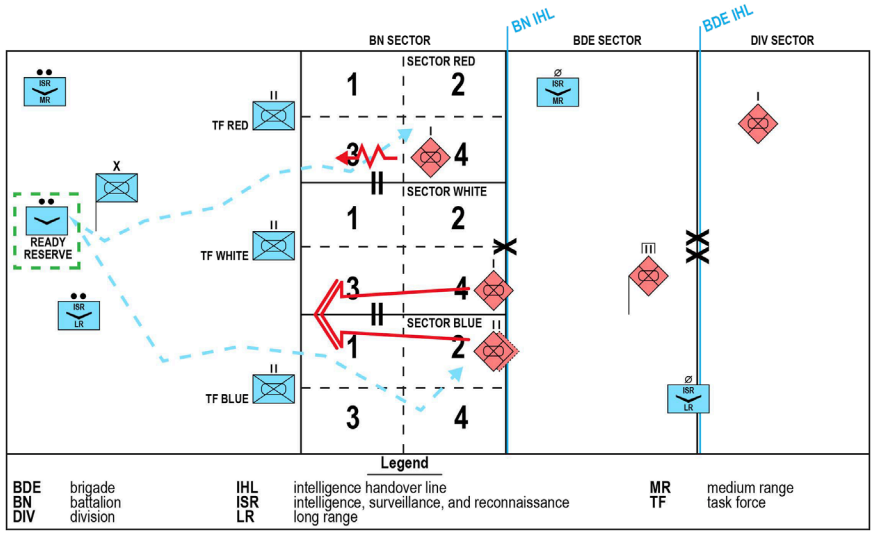


Figure 2. Ready Reserve Concept

A 3rd Brigade, 10th Mountain Division Soldier conducts security at Hohenfels Training Area, Joint Multinational Training Center, Germany, January 30, 2025. (U.S. Army Reserve photo by SSG Miguel Miolan)

For instance, consider the previous scenario. Following the detection of enemy elements in Sector Blue, the battalion's SUAS maintain persistent observation, confirming that the enemy is shaping conditions for a breach. As two mechanized enemy companies mass at the boundary between Sector Blue 2 and the battalion intelligence handover line, Task Forces Blue and White identify indicators of a coordinated penetration attempt.

Despite maintaining ISR coverage within its sector, Task Force Blue's organic SUAS are already fully tasked. To address the threat without stripping coverage from other sectors, the brigade collection manager activates the Ready Reserve. The Ready Reserve rapidly launches additional drones to reinforce surveillance in Sector Blue and extend observation into the adjacent brigade sectors.

As these reserve drones begin tracking follow-on enemy echelons along a concealed route, the intelligence section directs the cueing of mid-range reconnaissance SUAS to extend depth and maintain continuous custody. Fires and maneuver elements adjust their disposition based on real-time imagery and target confirmation. The ability to surge SUAS from the Ready Reserve enables the brigade to maintain situational awareness, support fires coordination, and deny the enemy freedom of movement—all without degrading the ISR posture in other sectors. This capability challenges the traditional tenet of "no reconnaissance in reserve." The Ready Reserve SUAS are best viewed not as assets to be conserved , but as a force ready to be committed to gain and maintain contact with the enemy.[8]

Transforming Collection Management in Contact

One of the primary challenges to fully operationalizing a SUAS framework is the brigade collection manager's limited, often reactive role. Many collection managers today focus on tasking and asset allocation but lack the training to integrate SUAS into operational planning and maneuver synchronization.[9] This reactive posture results in drone missions driven by immediate requests rather than proactive collection plans, perpetuating the enduring dilemma of "fighting the plan, not the enemy."

To meet the demands of modern warfare, the collection manager must evolve from a platform allocator into a force enabler—one who drives collection by managing effects and capabilities as integral components of operational design. The brigade collection manager's span of control is limited; this requires collection managers at all echelons to prioritize establishing a clear commander's intent and enabling subordinate battalions to independently plan and execute SUAS missions that support the brigade's objectives.

The collection manager of 2030 must possess a unique blend of technical expertise, operational awareness, and doctrinal fluency. Courses like the Information Collection Planners Course are essential, but collection managers must also develop a deep understanding of SUAS employment—specifically the range, payloads, and limitations that shape tactical options. This role also exceeds the capacity of a single individual. Dedicated collection management teams at brigade and battalion levels are essential for distributing responsibilities between current and future operations to ensure continuous support, proactive planning, and timely employment of collection assets.[10]

For this framework to succeed, collection management teams must integrate with maneuver units throughout training, rehearsals, and

execution. Integration of SUAS should be a core element of operational planning, enabling SUAS to function as organic extensions of maneuver forces for target development, reconnaissance, deception, and force protection. During operational planning at the brigade and battalion levels, intelligence sections should proactively recommend how to maximize SUAS employment to commanders and operations elements.

Consider a scenario where the brigade's objective is to attack and seize key terrain held by a degraded enemy force in hasty defensive positions. The enemy consists of two mechanized infantry companies in the front, and one in the rear as a second echelon. Intelligence assessments indicate that the rear company lacks sufficient combat power to maneuver and has entrenched itself in a tactically advantageous position that could threaten friendly forces during their approach.

To mitigate this threat, the intelligence section proposes to the operations element that a portion of the SUAS assets be employed to fix the degraded enemy force. This can be achieved through a combination of drone sound propagation, one-way attack SUAS, and jamming, synchronized with a coordinated fires plan. By executing this plan, friendly forces can divert minimal combat power to fix the entrenched enemy, freeing maneuver elements to sustain the main effort and achieve a successful penetration and envelopment of the adversary.

This example illustrates how deliberate SUAS integration can enhance operational flexibility, maximize combat power, and create opportunities for battlefield success. Lessons from the Ukrainian conflict underscore the urgency of doctrinal adaptation to match the rapid pace of technological advancement. Integrating SUAS into traditional reconnaissance and operational

planning enhances decision making and creates new opportunities for ISR-driven maneuver warfare. However, success hinges on robust training, resilient communications, and a deliberate approach to integrating SUAS into tactical and operational frameworks.

At the center of this transformation is the evolving role of the brigade collection manager, who must shift from an asset allocator to a capabilities-and-effects integrator. The collection manager ensures SUAS operations align with the commander's intent, synchronizing real-time intelligence collection with maneuver and targeting to generate decision advantage in dynamic environments. Frameworks such as the Sector Collection Approach and Ready Reserve enable this integration, providing structured methods for SUAS employment that support reconnaissance, targeting, and strike operations. By leveraging these frameworks and embedding SUAS into doctrinal planning, training, and execution, brigades can achieve intelligence overmatch—empowering commanders with superior decision making, enhanced lethality, and operational adaptability on the modern battlefield.

Turning the Tide

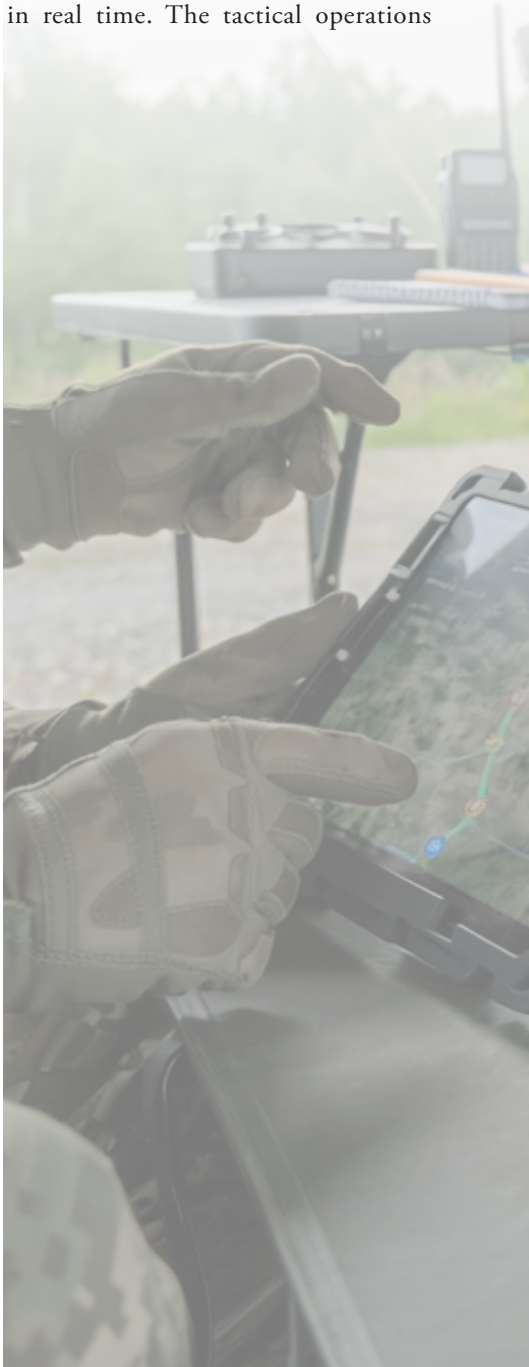
Author's note: This vignette is a fictitious representation of a nonexistent unit.

Kaptain Marchenko quickly leveraged the Sector Collection Concept, prioritizing critical zones near Chasiv Yar and along the surrounding ridgelines. Each grid received overlapping coverage tailored to terrain and threat indicators, enabling persistent and responsive intelligence collection.

Flying low and exploiting terrain for concealment, the SUAS network began to illuminate the battlefield. In one sector, drone feeds identified concealed mortar teams responsible for earlier indirect fire. In another, intercepted signals and thermal imagery revealed a Russian command post camouflaged within a cluster of abandoned buildings. The brigade's decentralized, but synchronized, plan allowed subordinate units to control their organic SUAS while remaining nested within the broader collection architecture, ensuring rapid exploitation of sensor data and reducing intelligence, surveillance, and reconnaissance latency.

As the intelligence picture developed, Marchenko identified a critical gap in the enemy's array—a seam between two Russian elements that left their flank exposed. Acting as the brigade's collection manager and subject matter expert, she immediately advised the operations officer and the commander that conditions had been met to transition from shaping to decisive action. She recommended employing the Ready Reserve, specifically its strike drone capability equipped with a first-person view, to fix the enemy in place and deny maneuver options. This would create conditions for committing Anvil Company, the brigade's reserve force, to exploit the gap and strike deep into the enemy formation, forcing an early culmination of the enemy's attack.

Moments later, a Ready Reserve drone confirmed the command post's location in real time. The tactical operations



center coordinated an immediate artillery strike, disrupting the enemy's ability to command and control. With their leadership node destroyed and forward elements disoriented, Ukrainian forces regained momentum and pushed through the ridge to secure Bakhmut. Deprived of coordination and overwhelmed by precision effects, Russian forces were forced into a hasty retreat.

Endpoints

[1]Dominika Kunertova, "Drones Have Boots: Learning from Russia's War in Ukraine," ***Contemporary Security Policy*** 44, no. 4: 576–91, https://doi.org/10.1080/13523260.2023.2262792.

[2]Jeffrey A. Edmonds and Samuel Bendett, "Russia's Use of Uncrewed Systems in Ukraine," Center for Naval Analyses, March 31, 2023, https://www.cna.org/analyses/2023/05/russias-use-of-drones-in-ukraine.

[3]Department of the Army, Field Manual (FM) 3-98, Reconnaissance and Security Operations (Government Publishing Office [GPO], 2023), 1-7..

[4]Anthony R. Padalino, "The Army Needs to Quickly Adapt to Tactical Drone Warfare," *Infantry* 113, no. 2 (2024): 32–36, https://www.benning.army.mil/infantry/magazine/issues/2024/Summer/pdf/10-Padalino_txt.pdf.

[5]Kerry Chávez and Ori Swed, "Emulating Underdogs: Tactical Drones in the Russia-Ukraine War," Contemporary Security Policy 44, no. 4, 592–605, https://doi.org/10.1080/13523260.2023.2257964.

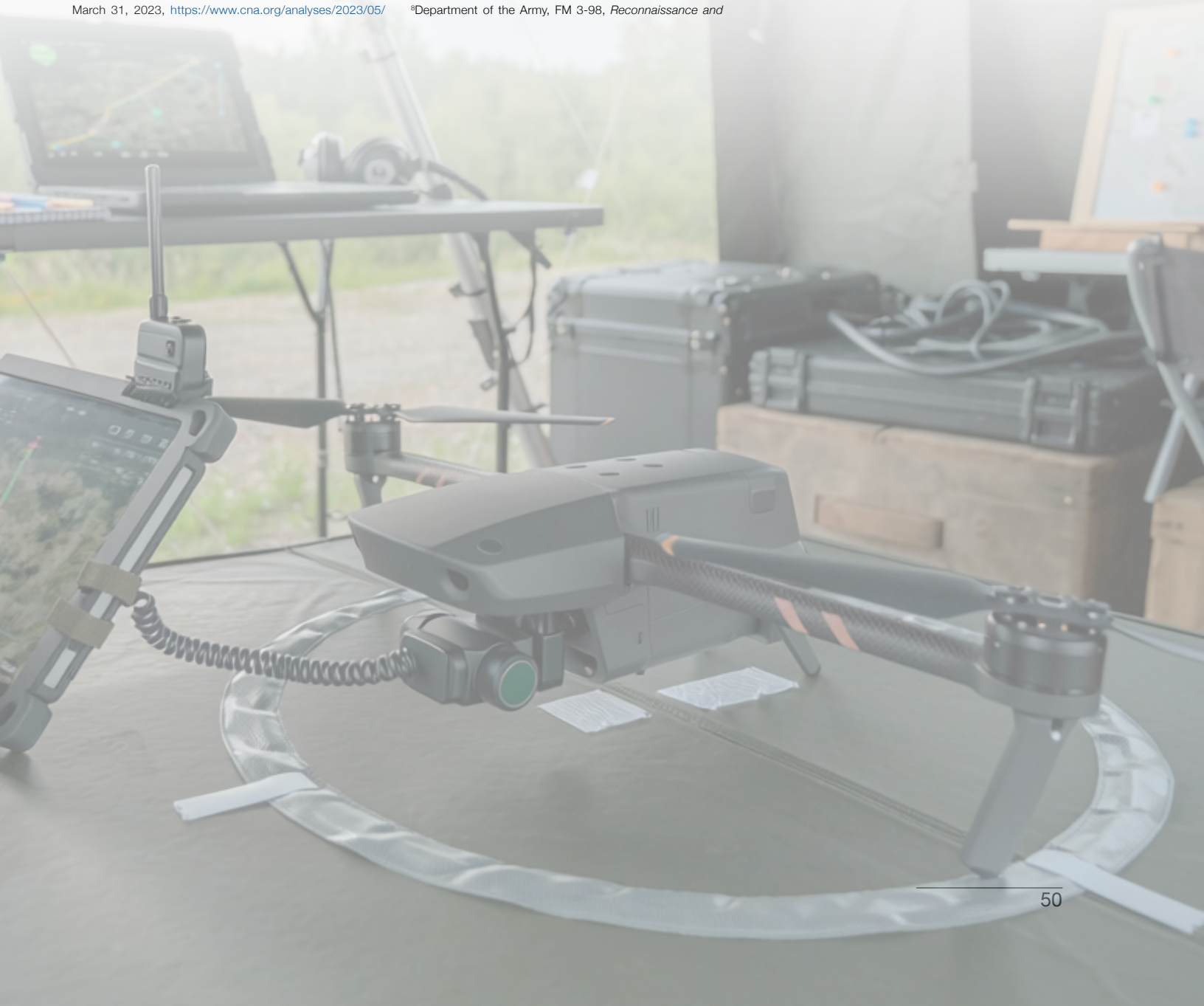
[6]David Hambling, *Swarm Troopers: How Small Drones Will Conquer the World* (Archangel Ink, 2015).

[7]Department of the Army, Army Techniques Publication (ATP) 2-01, Collection Management (GPO, 2021), 5-3. Incorporating change 1, September 2025.

[8]Department of the Army, FM 3-98, *Reconnaissance and Security Operations*, 4-1.

[9]"Matthew F. Smith, "Enabling Success of Brigade Combat Team's Collection Management in the Era of Multi-Domain Operations," *Military Intelligence Professional Bulletin* 47, no. 1 (2021): 69–76, https://mipb.ikn.army.mil/media/maaf330m/mipb-2021-01-03-full-issue.pdf#view=fit&page=71.

[10]Department of the Army, ATP 2-01, *Collection Management*, 1-2.



Corrected article from the previous Volume 14, Issue 1:

The Intelligence Warfighting Function as it Relates to Cyber. Is it Different?

By CW4 Michael Lewis, battalion senior technical advisor, 781st Military Intelligence Battalion (Cyber)

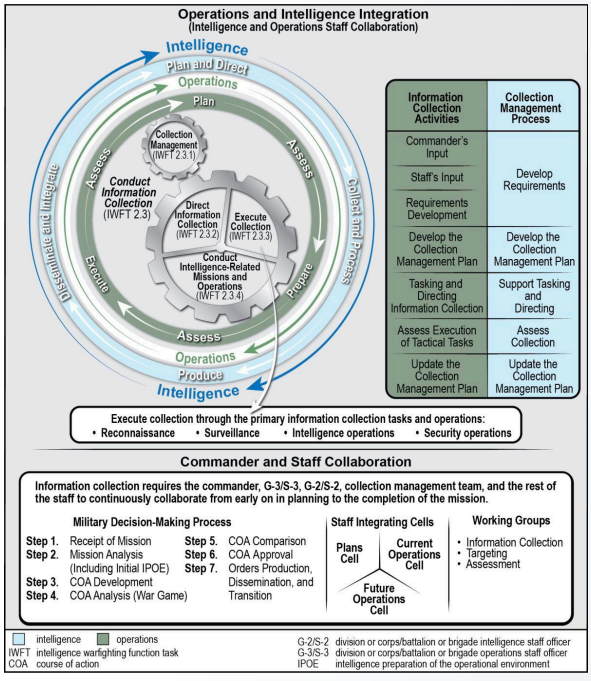
OVER THE YEARS, there seems to be a lot of speculation and rumors about what intel support to cyber looks like. What is in the realm of possible? How does intel support to offensive cyber differ to intel support to defensive cyber? Is it different?

For me, prior to arriving to the 781st in 2021, I had no operational cyber domain experience. Sure, like a lot of folks in this organization, I had some COMPTIA certs and had some college courses in information technology and cybersecurity. Did having those classes matter in the grand scale of intelligence support to cyber? I don't think it did. I believe it helped with learning the vernacular enabling communication with cyber focused people. It helped me understand the nuances of a cyber scheme of maneuver versus a traditional ground component kinetic operation scheme of maneuver. But honestly, I don't believe it really mattered. While intel support to cyber is highly nuanced, I do not believe the nuance is so dramatic that it changes the functions of intel support. When it comes down to it, intelligence provides support to operations, both kinetic and non-kinetic.

What is the Intelligence Warfighting function? FM 2-0 (Intelligence), paragraph 1-21 states, "Intelligence is one of the warfighting functions that enables the Army to generate combat power during the conduct of operations. The *intelligence warfighting function* is the related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment." During my time as a 35N/352N, having supported Tactical, Operational and Strategic level operations, I can attest the Intelligence Warfighting Function does not change no matter the echelon or type of mission it applies to. Each mission is nuanced. That nuance is based upon the Commander's requirements and end-state of the mission. This is the foundation of intel support.

If you look at Cyber as maneuver, the same foundation applies. I like to say, "Cyber is a tactical action arm with strategic level effects." It requires deliberate planning at strategic and operational levels to identify legitimate end goals. You must understand the operational environment, identify gaps, conduct collection management, collect, process, analyze, and disseminate information to support the operation. To do this, it requires deliberate planning at strategic and operational levels and coordination, collaboration, and constant communication between the S/G/J-2 and the S/G/J-3 to ensure the mission is in line with current approved authorities and meets the commander's intent.

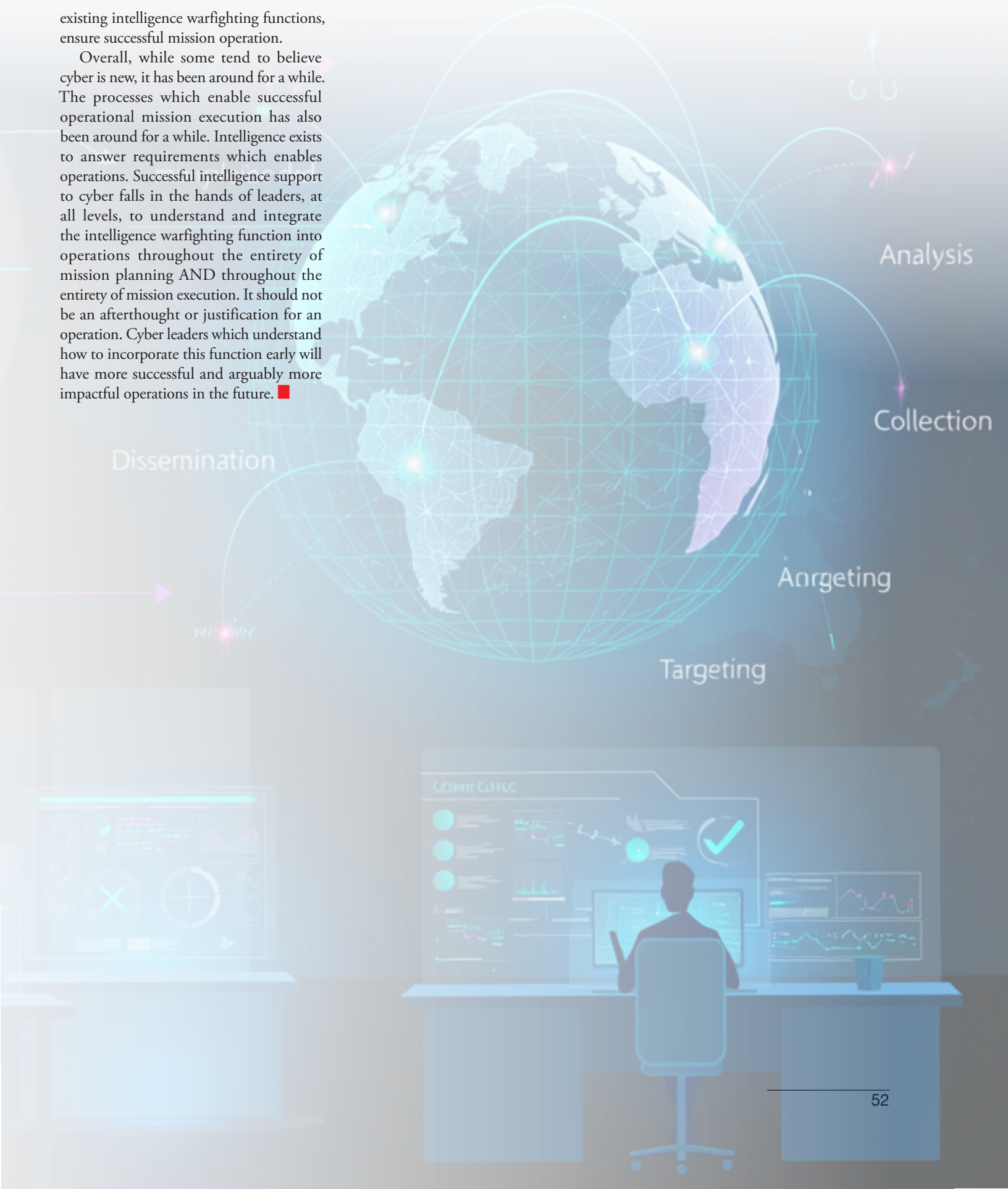
The intelligence warfighting function starts with "plan and direct." This requires commander's input in the form of requirements and orders. From a staff perspective, this function is where the Commander's Priority Intelligence Requirements (PIR) are developed and approved. This will drive collection management and separate mission elements to conduct further coordination and planning to request information and decide how to delegate tasks to complete the process. From the Intelligence Analyst perspective, you take commands from the tower and work to conduct the intelligence process (Collect and Process, Produce, Disseminate and Integrate). It is the integration of the intelligence you produce which will answer the commander's PIRs. It takes the collective actions of individual analysts, teams, and staff, utilizing the

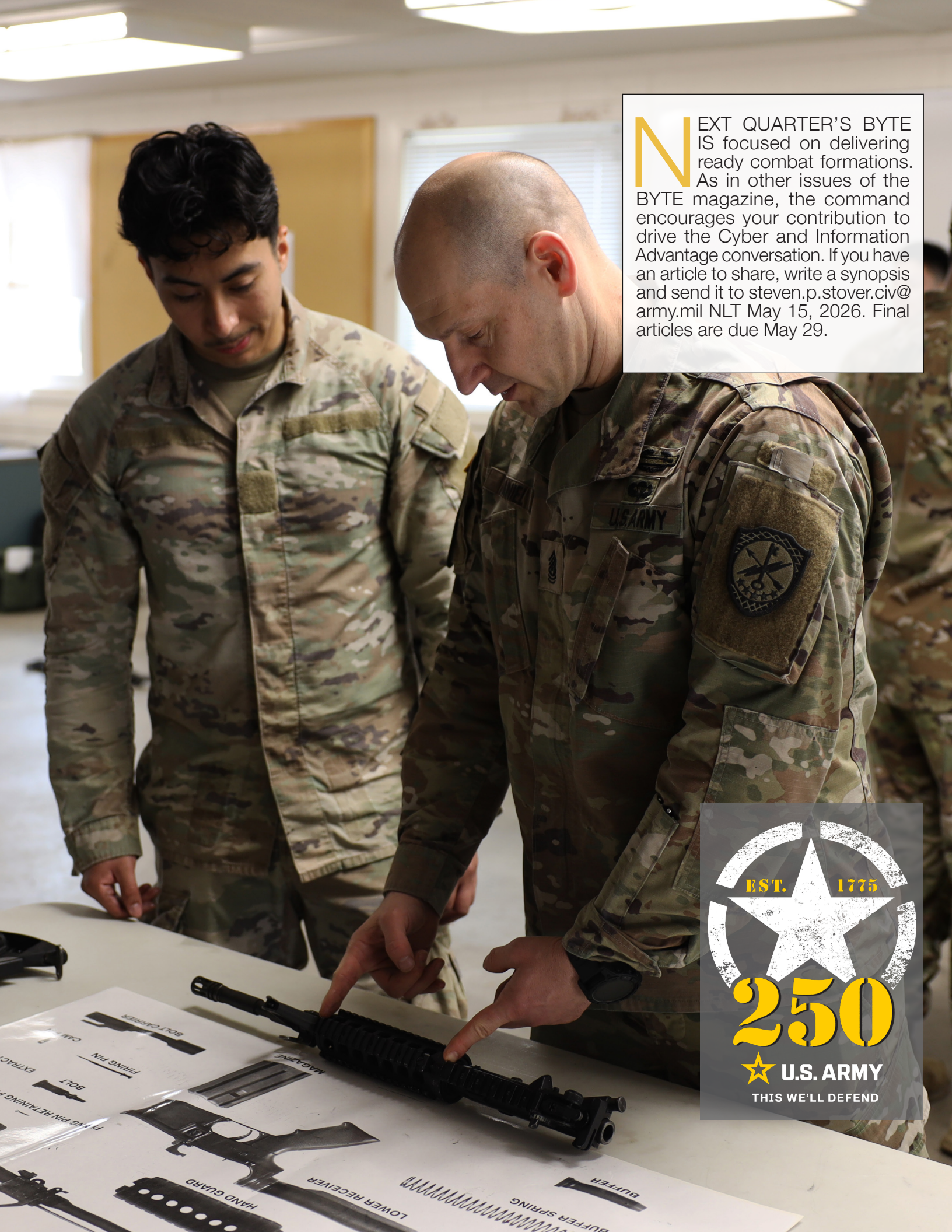


The above graphic from FM 2-0 highlights what collaboration would look like between the intelligence process and S/G/J-2 and the S/G/J-3 agnostic of the type of effect the mission is working to accomplish.

existing intelligence warfighting functions, ensure successful mission operation.

Overall, while some tend to believe cyber is new, it has been around for a while. The processes which enable successful operational mission execution has also been around for a while. Intelligence exists to answer requirements which enables operations. Successful intelligence support to cyber falls in the hands of leaders, at all levels, to understand and integrate the intelligence warfighting function into operations throughout the entirety of mission planning AND throughout the entirety of mission execution. It should not be an afterthought or justification for an operation. Cyber leaders which understand how to incorporate this function early will have more successful and arguably more impactful operations in the future. ■





NEXT QUARTER'S BYTE IS focused on delivering ready combat formations. As in other issues of the BYTE magazine, the command encourages your contribution to drive the Cyber and Information Advantage conversation. If you have an article to share, write a synopsis and send it to steven.p.stover.civ@army.mil NLT May 15, 2026. Final articles are due May 29.