

BREAKING DEFENSE

DISA
Dashboard

E-BOOK:

A New Age for DoD Networks and Cyber

SPONSORED BY

LUMEN®

Note from the Editor

One of the key takeaways from the conflict in Ukraine is that any combat operation, offensive or defensive, is going to fail or succeed on the ability to provide modern command and control. At this year's AFCEA TechNet conference, that was on full display — as was the wide variety of technologies that can play into the concept of C2 in 2023.

Artificial intelligence was a major focus of the show, as the role of publicly available AI's like ChatGPT had just exploded into mainstream discussion. The ability to quickly upgrade software was another hot topic, as the cat-and-mouse game on the modern battlefield requires constant updates. And hanging over the whole show is the question of China, America's "pacing threat" and the driver behind the Pentagon's investment in new technologies.

The coverage you'll find in this eBook runs that gamut and helps fill in the details. But it's an ever evolving story, so make sure you regularly check BreakingDefense.com for more cyber, IT and network news from the world of defense.

Thanks for reading,

Aaron Mehta
Editor in Chief, Breaking Defense



Table of Contents

DISA embarks on new reshuffle to better align to China threat	4
Keep moving or die: Army will overhaul network for rapid maneuver in big wars	6
'Like Netflix': After slow start, Army aims to 'drastically' accelerate software updates	9
Pentagon chief AI officer 'scared to death' of potential for AI in disinformation	12
Zero trust 'sure as heck' might have helped stop Discord leaks: Pentagon CIO	14
Military cyber directors: Help us better leverage AI to gain the 'high ground'	16

DISA embarks on new reshuffle to better align to China threat

“We decided to go with J codes for the fact of better aligning with our combatant commands, better aligning with the Joint Staff, and as a Combat Support Agency, it just makes sense,” Lt. Gen. Skinner said.



Lt. Gen. Robert J. Skinner, seen in a 2018 photo, is now the head of DISA. (U.S. Air Force photo by J.M. Eddins Jr.)

By JASPREET GILL - May 08, 2023

TECHNET CYBER 2023 — The [Defense Information Systems Agency](#) (DISA) is set to begin a wave of reorganization that the agency’s chief says will help it keep up with strategic threats — specifically from China, America’s top competitor.

“So as we look at the China threat, and as we look at the strategic threats out there, we did some analysis and some internal looks [and] we weren’t functionally aligned optimally,” [Lt. Gen. Robert Skinner](#), told reporters May 3 at the [AFCEA TechNet Cyber](#) conference in Baltimore.

“And so as we looked at how do we function...optimally, that’s really what this was all about,” he continued. “Whatever we call it is secondary to making sure that we are functionally aligned so that we have experts in charge of a particular functional area that can get after that mission function...of that organization.”

“We decided to go with J codes for the fact of better aligning with our combatant commands, better aligning with the Joint Staff, and as a Combat Support Agency, it just makes sense,” Skinner said. The agency will begin its first “major movement” next month, Skinner told reporters.

As part of the new reorganization, DISA will have a J-1 solely focused on human resources and a brand new J-2 “intelligence function” for the agency.

“The agency has never had one before,” Skinner said about the new J-2 during his keynote speech at the conference. “And so there will be an intelligence organization that is solely focused on providing the intelligence needs for the agency. There will be a J-3,5,7 in charge of ops, plans and exercises. Very typical of a J-3, 5, 7.”

There will also be a J-4 focused on warehousing logistics facilities; a J-6 that will bring together DISA’s Endpoint and Customer Service Directorate and the Joint Service Provider; a J-8 focused on requirements and finance; and the agency’s Host and Compute Center will be the agency’s J-9, Skinner said. At the end, the agency will have program executive offices “that are aligned with delivering capabilities.”

This is the second major reorganization of DISA under Skinner, who in 2021 said the agency’s organizational structure was too complicated. Under that previous shuffle, the agency moved from two main centers to four centers to more closely align with its strategy: the first center was focused on enterprise capabilities and security, the second center was focused on hosting and computing, the third was focused on operations and infrastructure and the fourth center was focused on innovation, [C4ISRNET reported](#).

Keep moving or die: Army will overhaul network for rapid maneuver in big wars

The Army has nixed future “Capability Set” upgrade packages for brigade networks in favor of smaller, more frequent updates, with the most complex technology reserved for division and corps HQs.



Maj. Gen. Jeth Rey briefs reporters at Fort Myer in May 2023. (Sydney J. Freedberg Jr. photo for Breaking Defense)

By SYDNEY J. FREEDBERG JR. - May 05, 2023

FORT MYER, Va. — As [ceremonial cannons](#) boomed intermittently in the distance, the two two-star generals tasked with modernizing the Army’s combat networks laid out how the [lessons of Ukraine](#) are forcing the service to speed up — both in acquisitions and on the battlefield.

“We need to be on the move,” said [Maj. Gen. Jeth Rey](#), head of the [Network Cross Functional Team](#) at Army Futures Command. If US Army units, as currently equipped and organized, had to fight a high-intensity conventional conflict like the one ongoing in Iraq, their large and slow-moving headquarters units would be located by enemy drones or electronic sensors and struck by long-range missiles, rockets, or cannon fire in “minutes” of stopping to set up their communications gear.

“We don’t believe that their command posts are going to survive,” Rey said. “We can’t halt” to set up radio antennas and get connected to the network. Instead, the service needs command posts that can stay connected and communicate continuously while on the move.

That kind of mobility may require slimming down the complexity and capability of network equipment in smaller, front-line units like battalions and even brigades, said Rey and [Maj. Gen. Tony Potts](#), the Army’s acquisition Program Executive Officer for tactical communications (PEO-C3T). The generals spoke at a briefing for reporters during a demonstration of Army communications tech.

One big example: classified networks. Today, Potts explained, units as small as front-line battalions — as few as 400 soldiers — are equipped with the [Command Post Computing Environment](#), which requires bulky “tactical servers.” But if you want more mobile battalions, and you’re willing to let them rely on higher headquarters for some functions, “do you really need that level of command post computing inside a battalion formation?” he asked. What if you gave battalions smaller, cheaper systems available on the civilian market, networks not certified to handle classified data but still using robust “commercial standard encryption” — a standard known as “Secure But Unclassified – Encrypted” (SBUE).

Yes, Potts said, going unclassified might increase the risk the enemy decrypts your communication. So what? Tactical data is pretty perishable, he argued, especially if you keep moving. By the time the enemy intercepts, decodes, and analyzes your plans, you’ve already executed them; by the time he’s deciphered your location, you’re no longer there. “Even though there’s data out there, I’m moving so fast that by the time anyone gets through the encryption... it’s not useful to them anymore,” he said.

This kind of high-speed, stripped-down command would be a major change for a generation of officers who grew up in Afghanistan and Iraq, waging guerrilla warfare village by village and block by block under the watchful eye of well-equipped but largely stationary brigade HQs. Decades-long deployments against poorly armed enemies let the US build up elaborate bases with air-conditioned command posts where colonels could watch their subordinates on live drone video. But against an enemy like Russia — let alone China — well-endowed with drones and missiles, such static headquarters would be big, easy targets.

Yet, at the same time, the scale of such a great-power conflict would be so large, with tens of thousands of troops fighting over hundreds of square miles, that even a big brigade HQ would be too small to coordinate effective operations. (It’s even harder if you’re trying to coordinate not just ground troops but also air, sea, space, and cyber efforts, using what the Pentagon calls [JADC2 networks](#).) Instead, the Army is reorganizing its forces to reemphasize larger formations like the division, the corps, and even theater. That means those units’ HQs are getting new capabilities, from long-range artillery to big-data AI analytics to high-frequency radios capable of transmitting messages over 4,800 miles, as tested in the recent [Balikatan](#) exercise in the Philippines.

While all HQs will be beefed up, Potts and Rey explained, the network modernization scheme will now be “division-centric.”

That means, the two generals revealed, that the Army must move on from the current system of “Capability Sets,” which are basically brigade-sized packages of hardware and software that are updated every two years.

The service has already rolled out [Capability Set 21](#), which was designed for [light infantry brigades](#); it’s now fielding [Capability Set 23](#), which focuses on [Stryker brigades](#) of medium-weight, wheeled armored vehicles. It had been working on [Capability Set 25](#), which emphasized [heavy brigades](#) of tracked armor, and even [asking industry](#) about a potential Capability Set 27.

But now CS 25 and 27 are going away, Potts said: “You really won’t hear us talk about it that way.” Instead of biennial brigade-sized update packages, he said, the service will issue updates more frequently, with a particular focus on the division level. (This is part of a wider Pentagon push to move from multi-year, rigidly sequenced “waterfall” software development to the rapid update cycles known as “[agile](#)” development).

To ease the speedier updates, Potts added, the service is studying new ways of contracting and structuring acquisitions, such as the streamlined [Software Pathway](#). It also wants to move away from complex, tightly integrated systems to a more flexible format, where the Army as a whole uses a single, standardized software foundation but individual units can custom-build specific applications for their unique missions.



Maj. Gen. Tony Potts and Maj. Gen. Jeth Rey brief reporters at Fort Myer in May 2023. (Sydney J. Freedberg Jr. photo for Breaking Defense)

Especially for software, this decoupled approach should let units update the individual apps quickly, like updating apps on a smartphone, since each app is relatively simple and, if it crashes, it doesn't take the whole system with it. "As long as I'm not messing with the core software," Potts said, "and what I can build is an application or a plug-in that sits on top of it, I don't have to take it back to testing" every time a new update comes out. It should even be possible to send out updates and patches over a wireless network, the way commercial software companies do, instead of physically bringing in each radio and laptop for a hands-on overhaul.

Speeding updates is another reason to go for Secure But Unclassified – Encrypted, Potts explained. A network rated for classified data has to be tested more rigorously, typically by the [National Security Agency](#), which takes a lot more time.

None of this speed should come at the expense of "acquisition rigor," however, Potts emphasized. There will still be regular [Technical Exchange Meetings](#) with interested companies and biannual systems integration tests, he said, plus independent testing by the Pentagon's [Director of Operational Test & Evaluation](#) and full compliance with the [Clinger-Cohen Act](#).

That's a lot of tradeoffs to juggle, Potts acknowledged, and a lot of hard choices are still to come. "We're still in the honeymoon phase," he said with a laugh. "We're in the honeymoon phase until something happens that somebody doesn't like."

'Like Netflix': After slow start, Army aims to 'drastically' accelerate software updates

Today, just nine of the Army's 540 acquisition programs use the streamlined Software Pathway, but senior officials told Breaking Defense in an exclusive interview they aim to "exponentially" increase that number by the end of next year.



Army Futures Command's Software Factory operations taking place on March 22, 2021 in Austin, Texas. (U.S. Army Photo by Mr. Luke J. Allen)

By SYDNEY J. FREEDBERG JR. - May 04, 2023

WASHINGTON — After a sluggish start, the Army is slicing through self-imposed red tape so it can do faster software updates, which are essential to everything from payroll systems to cybersecurity to high-tech combat vehicles. The objective: remove a host of obstacles so the service can make widespread use of the streamlined [Software Acquisition Pathway](#).

SWP was created in 2020 to [bypass ponderous, industrial-age procurement processes](#) so the Pentagon could roll out new software at the same pace as the private sector, in weeks or months instead of years.

"We are embracing the Software Pathway," said Young Bang, principal deputy assistant secretary of the Army for acquisition. "We have the [legal] authorities to do that from Congress."

But the legal foundation by itself is not enough, Bang emphasized in an exclusive interview with Breaking Defense. There are plenty of regulations, bureaucratic processes, and plain old bad habits in the way.

"There's been institutional processes have been around for a long time for the DoD at large and the Army," he said. "Until you fix all those, we can't actually get to agile CICD [[Continuous Integration, Continuous Deployment](#)] releases every two-three weeks like Netflix."

"We're working on efforts to change that," he said.

"There's a lot of support within the Army and DoD to make that happen," added Jennifer Swanson, deputy assistant secretary for data, engineering, & software, speaking to Breaking Defense alongside Bang. "I honestly believe by the end of next year, we'll be in a much better place. We'll have a lot more flexibility to do what industry does."

For 3 Years, Slow Going

Right now, the service's software stats aren't that impressive. The number of Army programs using SWP has grown from one in 2020, when the pathway was first authorized, to nine — a dramatic increase but still less than 2 percent of the Army's 540 programs. Of those nine, officials told Breaking Defense, four are so new they're still in the planning phase and haven't yet delivered any actual software to users.

Of the five programs that are delivering usable software, just two are delivering updated code more frequently than once a year. The Army didn't provide more specific timelines, but that's a long way from commercial-style release cycles measured in weeks.

Besides the nine Army SWP programs, the service has another seven programs using a separate but similar congressional authority, known as the Budget Authority 8 (BA-08) [software pilot](#). These seven programs are all part of a larger Defense Cyber Operations (DCO) effort to shore up the service's cybersecurity — an area where rapidly evolving threats and the ever-changing digital landscape of the internet make swift updates especially essential.

The DCO programs are technically traditional [Major Capability Acquisitions](#), subject to an elaborate multi-phase process; but they've been given significant SWP-style flexibility, especially in the drafting of the formal requirements that their products must meet. So, while the Army didn't provide specific metrics on how fast DCO code is being updated, Young extolled them as "a huge success story."

There are also streamlined elements within other traditional software programs, such as IPPS-A, the service's new [Integrated Personnel & Pay System – Army](#) rolled out in January. Planned upgrades, originally envisioned as one massive package, will be subdivided into smaller, more manageable "chunks" that can be developed, tested, and rolled out much faster, Bang said.

Nevertheless, all these streamlined software efforts added together still amount to a rounding error within the Army's roughly \$40 billion annual acquisition budget. Bang, Swanson, and their staffs are striving to make SWP and SWP-like programs a much bigger piece of how the Army does business.

While there are just nine SWP programs now, "that number is growing rapidly," Swanson said. "Even this year, I honestly would expect it to close to double" as new programs ask to be on SWP from the beginning and existing programs ask to transition.

In the slightly longer term, "towards the latter part of '24, you'll see the numbers drastically improve," Bang told Breaking Defense. "You will see... a steady growth and then potentially an exponential growth."

Several different reforms give Bang and Swanson cause for their optimism. One, which applies across the Defense Department, is DoD acquisition chief Bill LaPlante's August 2022 edict [PDF] allowing "[defense business systems](#)" — such as payroll, contracting, or installation management — to use the Software Pathway. That significantly increased the number of programs eligible to escape the slow, traditional system into SWP.

Within the Army itself, they said, the service is working hard to streamline the requirements process. Traditionally, that takes years of [horse-trading between bureaucracies](#) to generate hundreds of pages of rigidly detailed specifications, which then can't easily be changed as technology improves, threats worsen, or users offer feedback. "A lot of times we develop software which we think is awesome, but people don't adopt it or use it," Bang said.

The Software Pathway, by contrast, allows programs to get underway with a much less detailed Initial Capabilities Document, setting broad-strokes requirements that can then be updated, expanded, and revised repeatedly throughout development. And, Swanson said, acquisition officials, Army Futures Command, and the service's Training & Doctrine Command (TRADOC) are now "working very closely" together to develop templates and other guidance to give programs a clearer path through the new process.

'Software Is Never Done'

Another major bottleneck is testing. Certainly, rigorous, realistic testing is important: Soldiers don't want communications networks crashing mid-combat, any more than they want their guns to jam or tanks to throw a track. But traditional Pentagon testing is built around complex, lengthy events that run through every aspect of a system. That's workable for hardware, which can't change rapidly once it's approved for fielding, but it's out of sync with how software updates work best, which require lots of quick, incremental changes. Most commercial software companies manage this by automating much of their testing: They use software to test their software, with algorithms running new code through routine checks at superhuman speed.

"We're working with ATEC so we [can] have automated testing," Bang said, referring to the independent Army Test & Evaluation Command. "That's a huge paradigm shift [and] they're completely on board." Instead of ATEC coming in at the end of a development cycle to manually retest the entire software package whenever any small change is made, they would instead get involved from the outset, access the outputs from the automated testing systems in near-real-time, and save their skilled human testers' time for the most important checks.

Figuring out how all this will work in practice is complex and time consuming, Swanson cautioned. But, she said, "by the end of '24, we will definitely have at least some of those software pathway systems that are able to automate testing."

Another huge institutional change is how the Army handles what it calls "sustainment." A traditional hardware program, like a truck or rifle, starts out in R&D, builds prototypes, goes through testing, and gets approved for fielding. Once fielded, the equipment may receive overhauls or upgrades from time to time, but day to day it's "in sustainment" and not expected to change, so it simply needs to be maintained and kept in working order. These functions are considered so different the Army actually has separate organizations for them, with the program managers who developed a new technology at some point handing it over sustainment officials.

But that hand-off doesn't work well for software, which requires constant updates to keep working properly. In effect, the "development" phase never stops, even after the software is fielded. So, starting in fiscal year 2024 (which begins Oct. 1, 2023), the Army will no longer move new software programs out of development into sustainment at all. Instead, authority of software programs — and the funding that comes with it — will stay with the same program management office that oversaw the initial R&D, allowing them to keep updating the code indefinitely.

"Software is never done," Bang said. That's actually a quote referencing the title of a landmark [2019 Defense Innovation Board study](#) that warned Pentagon software programs moved far too slowly because "DoD still treats software much like hardware."

In truth, though, the industrial-age development process doesn't even work for hardware anymore, because physical machinery increasingly depends on software. Even civilian cars now rely on digital tools for routine maintenance diagnostics, while military vehicles incorporate high-tech sensors, targeting systems, and even automated anti-missile defenses.

But while the Software Pathway is built for flexibility, it's not flexible enough that you can develop, say, a new tank or an aircraft carrier just using SWP. So, Bang and Swanson said, the Army is looking at splitting off the software portion of major weapons programs as a separate but intertwined acquisition, running rapid updates alongside the slower hardware development, with software and hardware using different processes.

[The service is already trying](#) this on a small scale with its Robotic Combat Vehicle experiment, where it has contracts with Qinetiq and Textron to build physical prototypes and a separate contract with [Applied Intuition](#) to build software development and testing tools.

In the longer term, Bang said, it [might apply the split approach](#) to the larger Optionally Manned Fighting Vehicle effort to replace the Reagan-era M2 Bradley armored troop carrier. Currently, multiple competitors are building rival prototypes, with each contender building a complete package of hardware and software. As OMFV matures, however, Bang said the service expects to split off an SWP to develop software in parallel to the hardware program.

"We're looking at embedding multiple pathways within each other...because software is now embedded in all of our platforms," Bang said. "As much as possible, we're trying to separate hardware from software, and data from software."

Pentagon chief AI officer 'scared to death' of potential for AI in disinformation

"Here's my biggest fear about ChatGPT," Craig Martell said. "It has been trained to express itself in a fluent manner. It speaks fluently and authoritatively. So you believe it even when it's wrong... And that means it is a perfect tool for disinformation..."



Department of Defense Chief Digital and Artificial Intelligence Officer Dr. Craig Martell spoke at the DoDIIS Worldwide Conference, Dec. 13, 2022, at the Henry B. Gonzales Convention Center in Texas. (DVIDS)

By JASPREET GILL - May 03, 2023

TECHNET CYBER 2023 — While the US military is eager to make use of generative artificial intelligence, the Pentagon's senior-most official in charge of accelerating its AI capabilities is warning it also could become the "perfect tool" for disinformation.

"Yeah, I'm scared to death. That's my opinion," Craig Martell, the Defense Department's [chief digital and AI officer](#), said today at [AFCEA's TechNet Cyber](#) conference in Baltimore when asked about his thoughts on generative AI.

Martell was specifically referring to generative AI language models, like ChatGPT, which pose a "fascinating problem": they don't understand context, and people will take their words as fact because the models talk authoritatively, Martell said.

"Here's my biggest fear about ChatGPT," he said. "It has been trained to express itself in a fluent manner. It speaks fluently and authoritatively. So you believe it even when it's wrong... And that means it is a perfect tool for disinformation... We really need tools to be able to detect when that's happening and to be able to warn when that's happening.

"And we don't have those tools," he continued. "We are behind in that fight."

Martell, who was hired by the Defense Department last year from the private sector, has [extensive AI experience](#) under his belt. Prior to his CDAO gig, he was the head of machine learning at Lyft and Dropbox, led several AI teams at LinkedIn and was a professor at the Naval Postgraduate School for over a decade studying AI for the military.

He implored industry at the conference to build the tools necessary to make sure information generated from the all generative AI models — from language to images — is accurate.

“If you ask ChatGPT ‘Can I trust you,’ its answer is a very long ‘No,’” he said to the audience. “I’m not kidding. It says I’m a tool and I’m going to give you an answer and it’s incumbent upon you to go verify it yourself. So my fear about...using ChatGPT, as opposed to fears about our adversaries using it... is that we trust it too much without the providers of the service building in the right safeguards and the ability for us to validate it.”

Martell’s warning comes as Pentagon leaders are anticipating ways to use generative AI for intelligence gathering and future warfighting. On Tuesday at the conference, Lt. Gen. Robert Skinner, director of the Defense Information Systems Agency (DISA), began his [keynote address](#) using a generative AI that cloned his voice and delivered his opening remarks.

“Generative AI, I would offer, is probably one of the most disruptive technologies and initiatives in a very long, long time,” Skinner said after revealing his introduction was AI-generated. “Those who harness that and can understand how to best leverage it, but also how to best protect against it, are going to be the ones that have the high ground.”

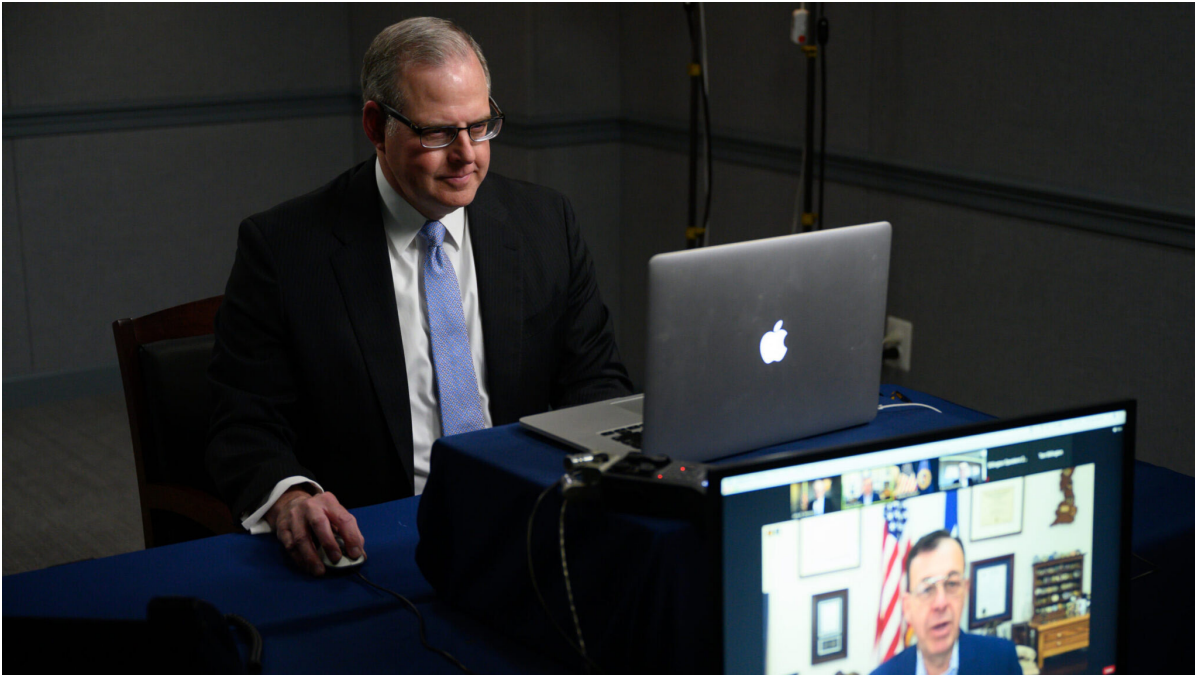
When asked today to respond to Martell’s thoughts, Skinner told reporters that he’s “not scared of generative AI,” but that it’ll be a “challenge to where the innovative spirit within the Department of Defense will shine.”

Stephen Wallace, DISA’s chief technology officer, said that the agency is looking at taking advantage of generative AI in several ways, from “back office capabilities... contract generation, data labeling.”

“The number of applications is very wide-ranging,” Wallace told reporters. “We always say that we can’t ‘people our way out of problems.’ And this is a way for us to augment our teams, make our teams better and ultimately deliver capabilities across the board.”

Zero trust 'sure as heck' might have helped stop Discord leaks: Pentagon CIO

A leak from a “trusted insider who has gone through the background investigation” and been given access to top-secret level capabilities is “a tough one that we have to be able to put measures to get after,” DoD CIO John Sherman said.



Mr. John Sherman, Acting Department of Defense Chief Information Officer participates in a virtual panel with Billington Cybersecurity at the Pentagon, April 15, 2021 (DoD photo by Chad J. McNeeley)

By JASPREET GILL - May 03, 2023

TECHNET CYBER 2023 — A full implementation of the Defense Departments zero trust strategy certainly might have helped prevent last month’s stunning leak of classified documents, according to the Pentagon’s chief information officer and the person ultimately in charge of keeping DoD data secure.

“I’ve seen in the tech media and the press and elsewhere different opining and stories about would zero trust have stopped this. I’ll tell you from my seat, I think it sure as heck would’ve made it a lot more likely that we would’ve caught this and been able to prevent it at the front end of something like this happening,” John Sherman told the audience at [AFCEA’s TechNet Cyber](#) conference in Baltimore.

Last month, Jack Teixeira, a 21-year-old member of the Massachusetts Air National Guard, allegedly [leaked](#) classified documents about the Russia-Ukraine war and several other topics on the social media platform Discord. Teixeira, who served as a “cyber transport systems journeyman,” held a top secret security clearance and maintained sensitive compartmented access, according to the [Department of Justice compliant](#) filed against him.

Although DoD officials [told Breaking Defense](#) following the leak that it was “too soon” to speculate on what preventative measures could have been taken to prevent the leak, Sherman said today that more focus needs to be placed on combating the threats from inside the department.

“We talk a lot about zero trust in terms of the global competition we’re in against state actors, People’s Republic of China and the PLA over there, Russia, Iran, North Korea,” he said. “But one of the most pernicious things we have to be aware of are insiders that will, using other means, release data that should never see the light of day in the way we saw here in this activity up at Otis Air Force Base.”

He added that a leak from a “trusted insider who has gone through the background investigation” and been given access to top-secret level capabilities is “a tough one that we have to be able to put measures to get after.”

“Another area we need to be conscious of is the balance of need to know with need to share... But particularly at the top secret level, where we have capabilities like [the governmental intranet] [Intelink](#), where we have large corpus of documents and information there, we want analysts who are working in the intel sections to be able to connect those dots, to be able to do the work they need to do,” Sherman said at the conference. “But we also need to have some sort of data access controls.”

Sherman’s comments echo a statement from David McKeown, DoD’s chief information security officer, who told Breaking Defense following the leak that “an insider threat with legitimate authorization and access to information remains one of the most — if not the most — difficult challenges in protecting information.”

To that point, DoD is pursuing specific areas of its zero trust strategy and implementation roadmap, Sherman said — like robust user activity monitoring at the top secret and secret levels. As DoD CIO, Sherman is also tasked with conducting the 45-day review lead by the undersecretary of defense for intelligence and security into security related to the link case.

Sherman last month also issued a new directive giving the CIO’s of the military services a month to certify that their systems and networks comply with DoD’s least privilege and security access controls, DefenseScoop [reported](#). He added today he wants to see the military services reach milestones outlined in DoD’s zero trust roadmap to fiscal 2027, the targeted date for implementing a baseline set of zero trust capabilities across the information enterprise.

Military cyber directors: Help us better leverage AI to gain the 'high ground'

In a sign of how ubiquitous AI has become recently, DISA Director Lt. Gen. Robert Skinner began his keynote not speaking himself, but with a generative AI that cloned his voice and delivered the start of his remarks.



Navy Commander Kevin Blenkhorn, a computer sciences professor at the U.S. Naval Academy, works with his Joint Services teammates during the U.S. Army's 'Cyber Center of Excellence' Tuesday, June 10. (Georgia Army National Guard photo by Staff Sgt. Tracy J. Smith)

By JASPREET GILL - May 02, 2023

TECHNET CYBER 2023 — The military services need to figure out how to better integrate and leverage disruptive technologies like [artificial intelligence](#) into data-driven decision making, and senior cyber officials said today they need industry's help to do it.

Using current technology right now, Lt. Gen. Maria Barrett, commanding general of [US Army Cyber Command](#), said that work is “tremendously complex.”

“Anything we can do to buy down that complexity by leveraging AI and [machine learning] would be absolutely fantastic and essential for, I think, the challenges that we face in the future,” she told the audience at the AFCEA's TechNet Cyber conference in Baltimore. “I think we have the underpinnings of starting to be able to take advantage of it from an Army cyber mission standpoint.”

The military services and, more broadly, the Defense Department have been [exploring](#) ways that AI can be used in the future. As a part of that push, DoD stood up the Chief Digital and AI Office and, in January, the Pentagon announced it [updated](#) its decade-old guidance on autonomous weapon systems to include advances made in AI.

In a sign of how ubiquitous AI has become recently, Director of the Defense Information Systems Agency Lt. Gen. Robert Skinner began his keynote not speaking himself, but with a generative AI that cloned his voice and [delivered the start of his remarks](#).

“Generative AI, I would offer, is probably one of the most disruptive technologies and initiatives in a very long, long time,” Skinner said after becoming himself again. “Those who harness that and can understand how to best leverage it, but also how to best protect against it, are going to be the ones that have the high ground.”

Skinner added DoD needs industry’s help in understanding how to leverage AI faster and better than adversaries, and to understand how AI can apply to cybersecurity, intelligence gathering and warfighting capabilities.

“So how do we have the protective systems, the security and the network capabilities to support protecting that data and support our folks?” he said.

Maj. Gen. Joseph Matos, deputy commander of the Joint Force Headquarters-Cyber (Marines) and Marine Corps Forces Cyberspace Command, echoed Skinner’s remarks, said industry can lead the way in sharing knowledge about disruptive technologies with the force.

“We all hear about it [AI], we see it, we use it, but we are nowhere near at the skill level that industry has when it comes to operating this technology to [its] best utilization, defending that capability, whether that’s cloud or...how we’re going to use AI,” Matos said today. “That’s where industry comes in and the knowledge that you all can provide us because...the military schooling system is, as you know, a long and arduous process and to change the programs of instruction takes millions of years and thousands of lives to do.”

Matos added that while AI is “still a very nascent technology,” particularly for the military, the services need to think about how to incorporate it in the most beneficial ways.