FEDERAL NEWS NETWORK

EXECUTIVE BRIEFING SERIES

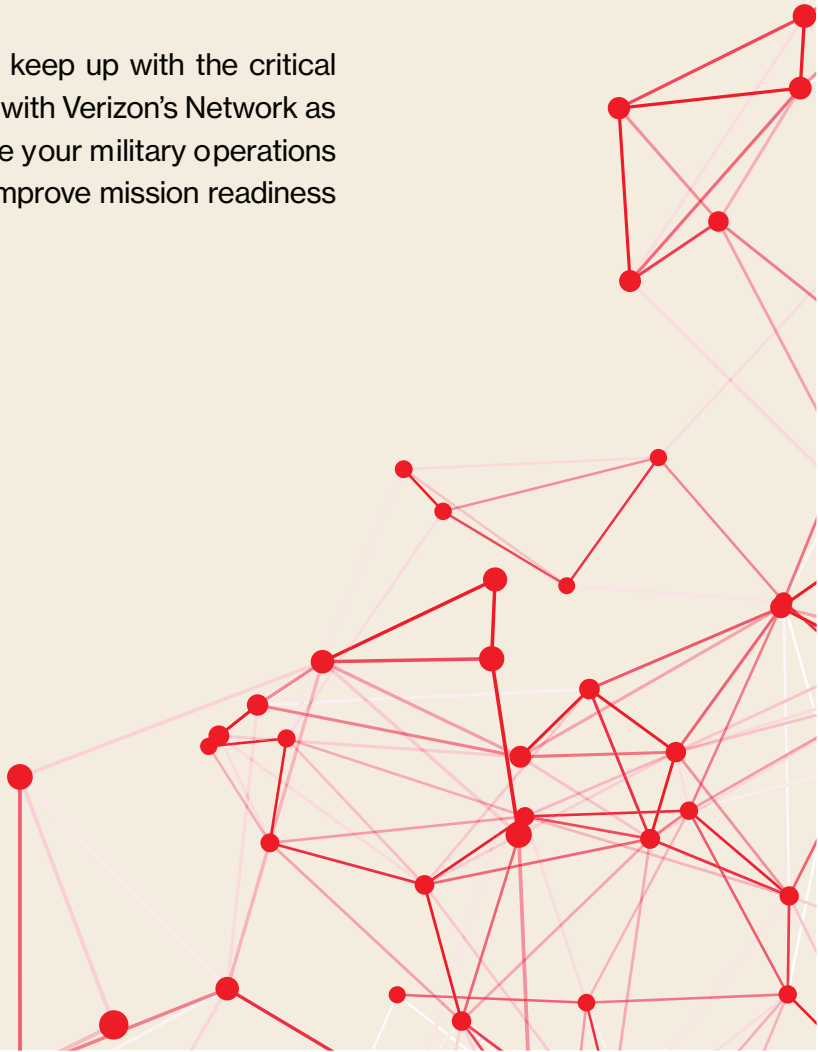
Threat hunters at the edge: How FEMA, DoD teams tackle cyber at frontline, disaster response sites

BROUGHT TO YOU BY verizon

It's time to upgrade your IT infrastructure.

We know you need the right network system to keep up with the critical communications challenges you face. Let us help with Verizon's Network as a Service. Our managed service offerings provide your military operations with a secure, scalable and virtualized network. Improve mission readiness today, with the network built for tomorrow.

Learn more at verizon.com



verizon

Threat hunters at the edge: Delivering cybersecurity to frontline and disaster response sites

BY DAISY THORNTON

Cybersecurity defenders on the front lines of the federal government, including those in the military and disaster response, face a massive increase in attacks directed at their networks by adversaries using increasingly devious tactics.

Artificial intelligence has been a driver, and federal cybersecurity teams across government have had to figure out how to respond with new tools and capabilities of their own. One way they're doing this is through increased connectivity and collaboration with partners inside the government and with foreign allies.

But to do that successfully, their highest priority has to be modernizing their own systems, so that they have the infrastructure to support new tools, capabilities and data-sharing techniques, said Lamont Copeland, senior director for federal solutions architecture at Verizon.

"If you're not doing the modernization of government networks, you're not going to be able to leverage the full capacity of all of the security capabilities to effectively protect government systems," Copeland said. "We're supporting the government

> **We're supporting the government in modernizing the network infrastructure and then we're moving up the networking stack.**
>
> — Lamont Copeland, Senior Director for Federal Solutions Architecture, Verizon

in modernizing the network infrastructure and then we're moving up the networking stack — supporting the modernization of voice, contact center and other enterprise services … and then layering on the security services."

That also involves services, such as software-defined wide area networks and secure access service edge solutions, to ensure Verizon is protecting not only the network assets but also the endpoint devices, applications and associated data as the enterprise is becoming more mobile and global, Copeland said.

Laying the connectivity foundation, integrating AI

Secure connectivity's especially important for the Department of Defense Information Network (DODIN), often touted as the biggest network in the world, with 3.5 million endpoints to defend on any given day. The network is so big that it was initially organized as a patchwork of loosely affiliated networks. There are just too many endpoints to directly control from a single vantage point.

Brig. Gen. James Hewitt, J3 deputy director of current operations at U.S. Cyber Command, said the maturity of adversaries' tactics, techniques and procedures led Cyber Command to organize DODIN into 45 sectors to facilitate defense at speed.

"The way that we defend is by pushing orders out, by pushing tasks and actions that we need our subordinate commanders to take in order to defend the network," Hewitt said. "Before, where it would take an order on any given day, three to five months to close — and by an order, I mean, 'Hey, take an action, go patch a box, go patch against a vulnerability' — we're able to do it at speed now. And so that's been pretty remarkable to see."

Cyber Command is also leveraging partnerships with other federal agencies, including law enforcement organizations like the FBI as well as foreign allies.

Hewitt called that an "asynchronous advantage" over cyber adversaries because while USCYBERCOM has many partnerships it can leverage, especially in information sharing, many adversaries work alone. They typically have no partners to collaborate with.

Meanwhile, Army Cyber Command (ARCYBER), a component of USCYBERCOM, focuses on the tools and capabilities to improve the military services' defense posture.

The command just recently rolled out a panoptic junction AI prototype, said Brig. Gen. Brian Wisniewski, mobilization assistant to ARCYBER's commander general.

We've been able to really highlight some of the areas where we had concerns, particularly across synchronization of our different regional cyber centers. Now, we can do cross-sector queries that allow the defensive cyber operations folks to be much more streamlined, much more organized in terms of how they approach the hunt missions.

— Brig. Gen. Brian Wisniewski, Mobilization Assistant to the Commander General, Army Cyber Command

"The goal of the prototype is really to focus in an automated way to interact with the Enterprise Mission Assurance Support Service and then leverage that in combination with cyberthreat intelligence," he said. "By doing that, we can begin to look at things at scale for both vulnerability management, risk management and session initiation protocol, or SIP, response."

Wisniewski said the prototype has been accepted by both ARCYBER and USCYBERCOM and will be used in response to the governmentwide AI executive order. U.S. Cyber Command will lead on that task — although ARCYBER will draft the report about the tool.

Bringing tools to 'disaster's edge'

For the Federal Emergency Management Agency, changes in its enterprise network changes are multiplying its challenges as it chases vulnerabilities and pursues patching. Its current focus is on delivering cyber to the "disaster's edge," said Greg Edwards, chief information security officer at FEMA.

FEMA has reached a level of maturity and compliance, especially regarding its Federal Information Security Modernization Act (FISMA) scores, which means it can start looking beyond the day to day and instead lean into deciphering cyberthreat intelligence.

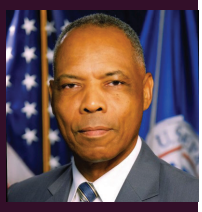
"We need to help ourselves focus a bit on what really matters, where threats are really, really severe. And we think cyberthreat intelligence will help us do

that," Edwards said. "We're building out our program in that regard. But it's all still, once again, about a disaster situation and the threat activity that's going on within that particular region or locality. We aren't on the front lines working directly with the mayors and governors, but we are coordinating in that regard."

That's where the collaboration comes into play for FEMA. Its teams need to be a strong partner to a variety of federal, state and local organizations in disaster response, he said.

We need to help ourselves focus a bit on what really matters, where threats are really, really severe. And we think cyberthreat intelligence will help us do that. We're building out our program in that regard.

— Greg Edwards, Chief Information Security Officer, Federal Emergency Management Agency



Cultivating cyber awareness

"Cyber risk tools are the next step after modernization, to help understand where all the data is moving and which end users are touching it," Copeland said. "The key is to understand where everything is and how it is all connected — to develop sound security protection solutions."

To that end, Wisniewski said his team recently finished an Army cyber data ecosystem inventory that included its military personnel, civilian employees and contractors, as well as other outside organizations. It provided insight into the service's cyber data rationalization efforts.

The data inventory focused on answering five questions:

1. What data does Army Cyber Command have?
2. Where is the data going?
3. What decisions are made with the data?
4. Who is using the data?
5. What are the data gaps?

"In doing that, we've been able to address some of the areas where we had concerns, particularly across synchronization of our different regional cyber centers," he said. "Now, we can do cross-sector queries that allow the

defensive cyber operations folks to be much more streamlined, much more organized in terms of how they approach the hunt missions."

Hewitt added that USCYBERCOM already has a host of cybersecurity tools. What it doesn't have is a capability for capitalizing on and federating the data, logging and scanning that happen across the networks. That's the current priority, which he called "battle space awareness."

"Really, what it is, is knowing your network, seeing a risk score down to the device by location so that we can decide where we want to focus our efforts because one gap in security is a gap for everybody and just provides an opening that adversaries can get in and pivot laterally to," Hewitt said.

The main issue USCYBERCOM has had so far is data standardization — getting all of its data in a standard format and then linking up all of DoD's big data platforms. That's been going well, he said, and the command is getting better at seeing everything across its networks.

To support efforts like this, "Verizon is currently building a management platform that can combine the tooling capabilities and security services that agencies need. That includes everything from security services using AI to compliance services using cyber risk tools," Copeland said.

> **We are … collaborating with agencies to modernize and protect their enterprises — no matter where they are in the world — in support of their missions.**
>
> — Verizon's Lamont Copeland

"Also, when agencies are getting network services from us, or any of our partners, we are building services like managed SD WAN in our government cloud platform and then collaborating with agencies to modernize and protect their enterprises — no matter where they are in the world — in support of their missions."

FEMA is also working to automate compliance and assessments to more quickly create essential documentation. That assessment data is then used to test the environment, look at the various controls in place from a management standpoint and really assess FEMA's security posture, Edwards said.

The agency wants to achieve a level of zero trust maturity that will balance mission with risk, he said. FEMA is calling its current effort a "cloud network security architecture," which will provide visibility into the devices on the network, the specifics on the data and all the communications occurring on the network.

Defending cyber forward

Edwards said that FEMA's big project right now involves sending cybersecurity advisors to established field offices dealing with disasters to advise its federal coordinating officers. They're the leaders in the field charged with coordinating between state and local officials, as well as FEMA and other federal agencies responding to a disaster. But they frequently don't have extensive cybersecurity knowledge, he said.

The forward defenders, these cybersecurity advisors, must be able to identify threat activity by sifting through all the regular network activity and then assess the risks and threats. That requires network visibility and tools that will let them quickly sort signals from the noise. Creating and fielding this type of capability is a priority for FEMA in 2025, Edwards said.

That's comparable to an effort currently being undertaken by the U.S. Cyber Command. The main distinction is that while FEMA's forward defenders report to field offices in disaster areas, USCYBERCOM teams often are situated with foreign allies to help them secure their networks.

That has a dual benefit, Hewitt said, of fostering international collaboration, as well as giving DoD's forward defenders a direct look at the tactics, techniques and procedures of adversaries against those foreign networks. The command may, for instance, get a first-hand view of new malware that they can bring back to study and train on.

"One example I'd like to highlight is a recent hunt forward that was completed in Ukraine where we were able to bring back 24,000 indicators of compromise — 3,000 of those were unique," Hewitt said. "We were able to turn those back over to our industry partners, which were then able to generate patching and software fixes and push that out — collectively securing the whole nation and not just our foreign partners."

Priorities on the horizon

USCYBERCOM's top priority is Cyber Command 2.0. It's a revamping of the model for the command established 10 years ago based on a template used by

the National Security Agency to meet the needs of the time. Now, the command is taking lessons learned from the past decade and applying them to determine a next-generation model that will serve DoD for the future.

"We're now at a point, thankfully, where we are manned and trained to a basic level," Hewitt said. "We've finished all our general education requirements in college, and now we're moving into grad school, and USCYBERCOM Command Gen. Timothy Haugh's focus has been on mastery now. How do we take the operators that we have on our teams and make them masters?"

ARCYBER is also focused on developing its personnel, Wisniewski said. The command wants to leverage its National Guard and Army Reserve personnel alongside its active component soldiers. That includes setting up opportunities for them in both mobilized and nonmobilized capacities. One example he mentioned is the National Guard State Partnership Program, which includes hunt forward operations.

Wisniewski also said that the Army Cyber Command Technical and Innovation Center will be part of efforts to turn cyber into a hybrid branch, with involvement in acquisition and development. That will be a collaborative area to bring public and private interests together along with academic institutions and research laboratories to focus on future needs.

Hewitt said a major effort moving forward for USCYBERCOM will be harnessing AI

One example I'd like to highlight is a recent hunt forward that was completed in Ukraine where we were able to bring back 24,000 indicators of compromise — 3,000 of those were unique. We were able to turn those back over to our industry partners, which were then able to generate patching and software fixes and push that out — collectively securing the whole nation and not just our foreign partners.

— Brig. Gen. James Hewitt, J3 Deputy Director of Current Operations, U.S. Cyber Command

to help spot "live-off-the-land" tactics by bad actors. That will involve analyzing millions of log entries to determine when authorized users on the network are doing things outside of their normal behavioral pattern and flagging that suspicious behavior for inquiries.

"A human can't really do that, and it's going to take forever to find it. I need artificial intelligence to tell me, to cue me, on that," Hewitt said. "Right now, even that's still a big lift. Three years from now, I think it'll be automatic. That's going to stop a lot of these living-off-the-land techniques because we're going to be able to catch unauthorized users masquerading as authorized users across the network and make ourselves a lot more secure."

That's something that Verizon is working to support too, Copeland said of using available data and AI capabilities to help secure federal networks.

"We're building in more AI capabilities to enable Verizon to do more automation of network security services, do more threat detection across the network and enterprises, and build in insights that can be leveraged both by Verizon security specialists and government agencies to protect their networks and end users." he said.

"We want to leverage the data available to provide more insights and create more actionable and automated services that will help protect government enterprises and support federal cyber missions."

How are DoD agencies collaborating to improve cyber and resiliency? Learn more now

And learn other ways that Verizon helps DoD revolutionize military operations. Discover more here

The sources in this article shared their comments during a Federal Executive Forum, presented by Trezza Media Group.