Persistent Engagement, Partnerships, Top Cybercom's Priorities

May 14, 2019
News
By C. Todd Lopez | Contact Author
Defense.gov

WASHINGTON -- As it embarks on its second year as a unified combatant command, U.S. Cyber Command is taking stock of its first year and looking toward the future.

Cybercom was created in 2008 as a subunified command under U.S. Strategic Command. On May 4, 2018, it became a full-fledged unified combatant command.

"We have an obligation to defend the nation, ensure the security of DOD information systems, and help joint force commanders achieve their missions," said Army Gen. Paul M. Nakasone, Cybercom commander, National Security Agency director and chief of the Central Security Service.

He called attention to how adversaries are undermining national security through incremental gains below the level of armed conflict.

"Through persistent presence, persistent innovation, and persistent engagement, we can impose costs, neutralize adversary efforts, and change their decision calculus," he said. "In doing so we build resilience, defend forward, and contest adversary activities in cyberspace."

Skip to main content (Press Enter).

Leaders at Cybercom expanded on how the organization has put that

strategy into practice.

“During the past year we’ve made a great deal of progress,” said David Luber, Cybercom’s executive director. “We were elevated to unified combatant command, [and] we’ve also deepened our partnership alongside theNSA. And thanks to Congress with the passing of the [Fiscal Year] 2019 National Defense Authorization Act, there’s been some new authorities that we’re also very happy about for the command, as well as some changes in presidential policy.”

Luber said Cybercom has been involved in “outstanding teamwork” across the DOD and with U.S. government and industry entities that has both been emboldened by its elevation to a unified combatant command, and helped it succeed as one.

Air Force Maj. Gen. Charles Moore Jr., the command’s director of operations, spelled out several focus areas Cybercom has pursued in its first year as a unified combatant command. Chief among those priorities, he said, is “persistent engagement” -- being fully engaged with adversaries in the cyber domain, full-time.

“We recognize and understand the importance of being in constant contact with the enemy in this space, especially below the level of armed conflict, so we can defend ourselves and impose cost,” Moore said.

Persistent engagement also involves persistent presence -- the sharing of information to enable partners -- and persistent innovation of technology and techniques with partners that include other government agencies, allied nations and industry, Luber said. Both are critical to Cybercom’s success as it moves into its second year.

Persistent Engagement With Persistent Force

“In the face of cyber threats, we’ve adjusted our strategic vision to one

"In the face of cyber threats, we've adjusted our strategic vision to one of persistent engagement with a persistent force," Luber said. "No longer reactive, but actually working in cyberspace in an area where there is no sanctuary or operational pause. It is the center of strategic rivalry in this era of renewed power competition. We are in constant contact with our adversaries. Success is determined on how we enable and act."

Getting outside of just U.S. networks and working with allies -- "defending forward" — is a second area of focus for Cybercom, Moore said. It's something lawmakers have enabled the command to do.

Changes to national policy and language in the 2019 National Defense Authorization Act, for instance, have in a limited way enabled Cybercom to step outside the Defense Department information networks and given it additional authorities to operate more effectively.

NDAA language, Moore said, declared cyberspace operations as a "traditional military activity." Without that, he explained, Cybercom would have to "declare or make very overt any of our operations, and acknowledge that it's being done by the DOD and the USA -- not very conducive to being successful inside the cyber domain. By declaring it a traditional military activity it allowed us to move away from that."

Focus on Readiness and Enabling Partners

Readiness is another top area of focus for Cybercom's leadership. Moore said the command at one point was focusing on building up cyber teams by manning and equipping them, but that work is largely over. Now, he said, they've moved into using those teams to operationalize the command.

"We've changed the readiness question from just building the teams to now, 'How do you work with the services, who of course organize, train

and equip our warfighting command ... to standardize what they are presenting in terms of people, in terms of how they are trained, in terms of the equipment they are presented to us with, so that we can sustain the readiness over the long term?'" Moore said.

Partnerships are a big part of what makes Cybercom successful, Moore said.

"There's probably not a greater team sport than cyberspace operations out there," he said. "We recognize we can't be successful in executing our mission against any of our adversaries if we are not working very closely with our interagency partners, with our friends and allies around the globe, with industry and academia, etc."

Today, the command partners with other federal agencies such as the Department of Homeland Security, Defense Intelligence Agency, Defense Information Systems Agency, the Energy Department and the FBI.

Last fall, DHS and DOD signed a memorandum of agreement to spell out how the two departments will work together to protect critical infrastructure.

"As the capacity in the department grows to be able to counter these malicious threats, how can that be brought to bear to defend the critical infrastructure?" asked Air Force Brig. Gen. Tim Haugh, Cyber National Mission Force commander. "We do that in lockstep with DHS."

During the 2018 midterm elections, Cybercom worked hand in hand with DHS and the FBI to defend election integrity. "Both of those organizations -- DHS and FBI — were really good teammates," Haugh said. What Cybercom learned working with DHS and FBI "has set a foundation for us as we look to 2020, which will certainly be an area where we continue to grow the partnership with DHS and the FBI and across industry to make sure we are doing our part in that role to

defend the electoral process."

Haugh said partnerships with industry have involved discovering new ways adversaries are exploiting the network and sharing that information with those most suited to develop countermeasures.

"We've done that by leveraging VirusTotal, which is a platform for sharing of malicious activity," he said. "We've taken malware we've found in the conduct of our operations and we've posted it directly to VirusTotal, with the goal of allowing industry then to quickly build countermeasures."

Fighting Election Interference

During the 2018 midterm elections, Cybercom partnered with allied nations, including Ukraine, Macedonia and Montenegro, to ferret out potential inference in the election process.

Were Cybercom to find election interference, Cybercom would not be responsible for directly notifying targeted candidates. The command would share what they found through established reporting channels. Haugh said that instead, the Office of Director of National Intelligence, DHS, or FBI would likely be involved in whatever notifications would be appropriate.

"Our goal is to have no interference in our elections," Haugh said. "We're going to support DHS and the FBI in the missions they've been assigned. But ideally, no foreign actor is going to target our electoral process."

And of course, the U.S. is partnered with traditional allies, including those that are part of "Five Eyes," including Australia, Canada, New Zealand, and the United Kingdom. The U.K. and Australia already have a presence on the Cybercom campus here.

Probably the most important partner for Cybercom, however, is the National Security Agency. Both agencies are located on the same campus and are led by the same person: Army Gen. Paul M. Nakasone, who serves both as NSA's director and as Cybercom's commander.

A recent cyber exercise, Moore said, revalidated "the importance of having unity of command by having one commander who runs both of those organizations.

Both organizations seeking to achieve the same overall outcome is a critical component of Nakasone's strategy.

"The partnership between U.S. Cybercom and NSA fosters speed, agility, and unity of effort," said Nakasone. "Addressing future cyber security challenges will require a whole-of-nation effort, to include both public and private sectors."

Innovation at Speed

In addition to building relationships and finding industry solutions for unique challenges, the command has several initiatives and capabilities that enable its agility and flexibility to innovate.

One of these initiatives is the Joint Cyber Warfighting Architecture, or JCWA.

"You notice it's not called a platform, because you can't buy one," said Army Maj. Gen. Karl Gingrich, the Cybercom director of capability and resource integration.

JCWA covers everything from access platforms where the command gains access to the internet, to data management, to command and control, to the tools they use during operations.

"We need to constantly innovate in this space because our adversary

gets a vote. So… we have to be adaptable to that," he said. "We are a learning organization across the Department of Defense and the Cyber Mission Force, so we have to have an architecture that is capable of allowing us to innovate and go where we need to go."

Gingrich also noted the importance of the Command's limited acquisition authority.

The authority gives Cybercom up to $75 million each year for its own procurement purposes in order to "meet the needs of our Cyber Mission Force through innovative acquisition and capability development."

U.S. Cyber Command