The Washington Post

Checkpoint

How the Pentagon’s cyber offensive against ISIS could shape the future for elite U.S. forces

By Dan Lamothe December 16

The U.S. military has conducted cyber attacks against the Islamic State for more than a year, and its record of success when those attacks are coordinated with elite Special Operations troops is such that the Pentagon is likely carry out similar operations with greater frequency, according to current and former U.S. defense officials.

The cyber offensive against ISIS, an acronym for the Islamic State, was a first and included the creation of a unit named Joint Task Force Ares. It focused on destroying or disrupting computer networks used by the militant group to recruit fighters and communicate inside the organization. Such offensive weapons are more commonly associated with U.S. intelligence agencies, but they were brought into the open in 2016 after then-Defense Secretary Ashton B. Carter pressured U.S. Cyber Command to become more involved in the campaign to defeat the Islamic State.

The move sparked a debate in the U.S. government over whether American allies would object to the U.S. military’s altering computer networks abroad, The Washington Post reported in May. Some intelligence officials argued that using such weapons in other countries could jeopardize the cooperation of international partners on which U.S. law enforcement and intelligence agencies depend.

But the cyber attacks were approved and launched anyway, and the campaign recently received the full-throated endorsement of Army Gen. Raymond A. “Tony” Thomas III, the head of U.S. Special Operations Command.

Speaking Wednesday to Army officers at a conference in Northern Virginia, Thomas cited Joint Task Force Ares, saying its efforts, combined with those of Special Operations troops, other elements of Cyber Command, the intelligence agencies and international partners produced “an operation which provided devastating effects on the adversary.”

When combined with traditional military operations, Thomas said, the cyber strikes culminated in the “destruction of that adversary on an epic scale.” He argued that the military can “only achieve exquisite effects like this” with a task force that combines a variety of capabilities, including cyber weapons.

“We should be conducting operations like this continuously in a campaign,” Thomas said. “We are not there yet, but we are trending positively in that direction, more every day.”

Thomas did not describe the operation in further detail. His spokesman, Navy Capt. Jason Salata, said he could not expand on the comments because of the operation’s sensitivity.

In May, Adm. Michael S. Rogers, who oversees U.S. Cyber Command, told the House Armed Services Committee’s subcommittee on emerging threats and capabilities that he created Task Force Ares to coordinate the efforts of Cyber Command with other U.S. forces in the fight against the Islamic State.

As The Post has reported, the campaign focused at least in part on preventing Islamic State propagandists from accessing their social media accounts by changing passwords. U.S. forces also deleted the Islamic State’s battlefield videos from the Internet.

Beginning about 13 months ago, personnel at Cyber Command’s headquarters at Fort Meade, Md., were said to have a leading role in the operation, although it is unclear how they integrated with forces from Special Operations Command or what the precise role of Special Operations Command was.

Thomas’s support for cyber operations is an encouraging sign, signaling that the military has overcome concerns within the intelligence community, said Eric Rosenbach, a cyberwarfare expert who served as Carter’s chief of staff during Carter’s tenure overseeing the Pentagon.

“It’s essential for the United States to use offensive cyber operations in a smart way against ISIS and other terrorist organizations because those organizations are so connected to the information environment,” Rosenbach said.

The mission Thomas described sounded like “exactly the type of operation that we should be doing,” Rosenbach said. Cyber Command, he added, will be more effective if it remains as agile as Special Operations Command and Joint Special Operations Command, the shadowy force that handles the military’s most sensitive missions.

“This was always our vision for Cybercom,” said Rosenbach, now co-director of Harvard University’s Belfer Center for Science and International Affairs. “We need a Cyber Command that is aggressive, dynamic and doesn’t think about cyber from the Cold War perspective of nuclear weapons.”

A spokesman for Cyber Command, Masao Doi, indicated that similar operations could occur in the future, saying Cyber Command learned through its campaign against ISIS how to integrate its specialized capabilities with a broader military campaign. And, he noted, “We do not anticipate that requirement diminishing now or in the future.”

James A. Lewis, who studies the intersection of warfare and the Internet for the Center for Strategic and International Studies, predicted a “wrestle for control” of cyber resources in the future.

“My concern,” he said, “is that Special Operations Command is very much in the anti-jihad campaign, and that may not be the strategic threat. … This isn’t the only thing Cyber Command needs to do.”

Ellen Nakashima contributed to this report.

6 Comments

Dan Lamothe covers the Pentagon and the U.S. military for The Washington Post. He joined the newspaper in spring 2014. Follow @danlamothe