The New York Times | http://nyti.ms/1SY7pYG

MIDDLE EAST

U.S. Cyberattacks Target ISIS in a New Line of Combat

By DAVID E. SANGER APRIL 24, 2016

LONDON — The United States has opened a new line of combat against the Islamic State, directing the military's six-year-old Cyber Command for the first time to mount computer-network attacks that are now being used alongside more traditional weapons.

The effort reflects President Obama's desire to bring many of the secret American cyberweapons that have been aimed elsewhere, notably at Iran, into the fight against the Islamic State — which has proved effective in using modern communications and encryption to recruit and carry out operations.

The National Security Agency, which specializes in electronic surveillance, has for years listened intensely to the militants of the Islamic State, and those reports are often part of the president's daily intelligence briefing. But the N.S.A.'s military counterpart, Cyber Command, was focused largely on Russia, China, Iran and North Korea — where cyberattacks on the United States most frequently originate — and had run virtually no operations against what has become the most dangerous terrorist organization in the world.

A review of what should be done to confront the Islamic State is on Mr. Obama's agenda on Monday, when he is scheduled to attend a conference in Hanover, Germany, with the leaders of Britain, France, Italy and

Germany. Of these efforts, the cybercampaign is the newest. It is also the one discussed in least detail by officials of many countries, and its successes or failures are the most difficult to assess from the outside.

The goal of the new campaign is to disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions, like paying its fighters. A benefit of the administration's exceedingly rare public discussion of the campaign, officials said, is to rattle the Islamic State's commanders, who have begun to realize that sophisticated hacking efforts are manipulating their data. Potential recruits may also be deterred if they come to worry about the security of their communications with the militant group.

Defense Secretary Ashton B. Carter is among those who have publicly discussed the new mission, but only in broad terms, and this month the deputy secretary of defense, Robert O. Work, was more colorful in describing the effort.

"We are dropping cyberbombs," Mr. Work said. "We have never done that before."

The campaign has been conducted by a small number of "national mission teams," newly created cyberunits loosely modeled on Special Operations forces.

While officials declined to discuss the details of their operations, interviews with more than a half-dozen senior and midlevel officials indicate that the effort has begun with a series of "implants" in the militants' networks to learn the online habits of commanders. Now, the plan is to imitate them or to alter their messages, with the aim of redirecting militants to areas more vulnerable to attack by American drones or local ground forces.

In other cases, officials said, the United States may complement operations to bomb warehouses full of cash by using cyberattacks to interrupt electronic transfers and misdirect payments.

The fact that the administration is beginning to talk of its use of the

new weapons is a dramatic change. As recently as four years ago, it would not publicly admit to developing offensive cyberweapons or confirm its role in any attacks on computer networks.

That is partly because cyberattacks inside another nation raise major questions over invasion of sovereignty. But in the case of the Islamic State, officials say a decision was made that a bit of boasting might degrade the enemy's trust in its communications, jumbling and even deterring some actions.

"Our cyberoperations are disrupting their command-and-control and communications," Mr. Obama said this month, emerging from a meeting at the C.I.A. headquarters in Langley, Va., on countering the Islamic State.

Gen. Joseph F. Dunford Jr., the chairman of the Joint Chiefs of Staff, offered broad outlines of the new campaign against the Islamic State, which is also known as ISIS or ISIL, during a news conference in February.

"We're trying to both physically and virtually isolate ISIL, limit their ability to conduct command and control, limit their ability to communicate with each other, limit their ability to conduct operations locally and tactically," he said.

"But I'll be one of the first ones arguing that that's about all we should talk about," General Dunford said. "We want them to be surprised when we conduct cyberoperations. And, frankly, they're going to experience some friction that's associated with us and some friction that's just associated with the normal course of events in dealing in the information age."

In an interview this month in Colorado Springs, where she talked to Air Force Academy cadets, Mr. Obama's national security adviser, Susan E. Rice, said that the fight against the Islamic State had to be thought of as a multifront war — and that computers were just another weapon in the arsenal.

"It should not be taken out of proportion — it is not the only tool," she said when asked about Mr. Work's "cyberbombs" comment. In fact, some of

Mr. Work's colleagues acknowledged that they had winced when he used the term, because government lawyers have gone to extraordinary lengths to narrowly limit cyberattacks to highly precise operations with as little collateral damage as possible.

But Ms. Rice said the Islamic State had "uniquely utilized cyberspace" to recruit, to communicate over encrypted apps and to coordinate its operations from Syria to Europe.

Ms. Rice would not comment on reports from officials in the Pentagon that Mr. Obama had asked — quite pointedly — in the fall why the arsenal of cyberweapons that had been developed at a cost of hundreds of millions, if not billions, of dollars was not being used in the fight against the terrorist group.

Several officials said that Mr. Carter had complained that Cyber Command was too focused on traditional adversaries, and that he had set deadlines for a new array of operational cyberplans aimed at the Islamic State. Those were ultimately delivered by Adm. Michael S. Rogers, the commander of Cyber Command and the director of the National Security Agency.

But inside Fort Meade in Maryland, home to the N.S.A. and Cyber Command, initial demands from the White House generated some resistance, according to officials involved in the debate.

The N.S.A. has spent years penetrating foreign networks — the Chinese military, Russian submarine communications, Internet traffic and other targets — placing thousands of implants in those networks to allow it to listen in.

But those implants can be used to manipulate data or to shut down a network. That frequently leads to a battle between the N.S.A. civilians — who know that to make use of an implant is to blow its cover — and the military operators who want to strike back. N.S.A. officials complained that once the implants were used to attack, the Islamic State militants would

stop the use of a communications channel and perhaps start one that was harder to find, penetrate or de-encrypt.

"It's a delicate balance," Ms. Rice said. "We still have to keep our eye on the Russia-China state-sponsored activity, but this was a new mission, one where we have to balance the collection equities against the disruption equities."

In Britain, the Government Communications Headquarters, the country's equivalent to the N.S.A., has been going through a similar debate. It is a familiar one for the British: According to an oft-repeated legend from World War II, Winston Churchill decided to let the Nazis bomb Coventry, at a cost of hundreds of lives, rather than reveal that Britain had used its Enigma machine to crack German codes. (There is a historical dispute about whether Churchill knew the city was to be targeted.)

Lisa O. Monaco, a deputy national security adviser and Mr. Obama's top adviser for counterterrorism, has led efforts examining how to disrupt the use of social media for recruiting. She has met technology executives in Silicon Valley; Austin, Tex.; Boston; and Washington to come up with a more integrated plan for both taking down social media posts and encouraging the development of a counternarrative.

One effort has included amplifying the testimony of Islamic State recruits who have escaped and now describe the group's brutality and question its adherence to the true tenets of Islam. Facebook, YouTube and Twitter are also growing more efficient at finding and removing Islamic State posts — which they can take down without court orders because the posts are a violation of the companies' terms of service, executives say.

But Ms. Monaco suggested that the effort was just beginning. "We are not going to kill our way out of this conflict," she said. "And we are not going to delete our way out of it, either."

A version of this article appears in print on April 25, 2016, on page A1 of the New York edition with the headline: U.S. Unleashes Digital Arsenal in War With ISIS.