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

MIDDLE EAST

Syria War Stirs New U.S. Debate on Cyberattacks

By DAVID E. SANGER FEB. 24, 2014

WASHINGTON — Not long after the uprising in Syria turned bloody, late in the spring of 2011, the Pentagon and the National Security Agency developed a battle plan that featured a sophisticated cyberattack on the Syrian military and President Bashar al-Assad's command structure.

The Syrian military's ability to launch airstrikes was a particular target, along with missile production facilities. "It would essentially turn the lights out for Assad," said one former official familiar with the planning.

For President Obama, who has been adamantly opposed to direct American intervention in a worsening crisis in Syria, such methods would seem to be an obvious, low-cost, low-casualty alternative. But after briefings on variants of the plans, most of which are part of traditional strikes as well, he has so far turned them down, according to officials familiar with the administration's long-running internal debate.

Syria was not a place where he saw strategic value in American intervention, and even covert attacks — of the kind he ordered against Iran during the first two years of his presidency — involved a variety of risks.

The considerations that led Mr. Obama to hesitate about using the offensive cyberweapons his administration has spent billions helping develop, in large part with hopes that they can reduce the need for more-traditional military attacks, reflect larger concerns about a new and untested tactic with the potential to transform the nature of warfare. It is a transformation analogous to what happened when the airplane was first used in combat in World War I, a century ago.

The Obama administration has been engaged in a largely secret debate about whether cyberarms should be used like ordinary weapons, whether they should be rarely used covert tools or whether they ought to be reserved for extraordinarily rare use against the most sophisticated, hard-to-reach targets. And looming over the issue is the question of retaliation: whether such an attack on Syria's air power, its electric grid or its leadership would prompt Syrian, Iranian or Russian retaliation in the United States.

It is a question Mr. Obama has never spoken about publicly. Because he has put the use of such weapons largely into the hands of the N.S.A., which operates under the laws guiding covert action, there is little of the public discussion that accompanied the arguments over nuclear weapons in the 1950s and '60s or the kind of roiling argument over the use of drones, another classified program that Mr. Obama has begun to discuss publicly only in the past 18 months.

But to many inside the administration, who insisted on anonymity when speaking about discussions over one of America's most highly classified abilities, Syria puts the issue back on the table. Mr. Obama's National Security Council met Thursday to explore what one official called "old and new options."

Caitlin Hayden, the spokeswoman for the National Security Council, declined to discuss "the details of our interagency deliberations" about Syria. "But we have been clear that there are a range of tools we have at our disposal to protect our national security, including cyber," she said, noting that in 2012 "the president signed a classified presidential directive relating to cyberoperations that establishes principles and processes so that cybertools are integrated with the full array of national security tools."

The directive, she said, "enables us to be flexible, while also exercising restraint in dealing with the threats we face. It continues to be our policy that we shall undertake the least action necessary to mitigate threats."

One of the central issues is whether such a strike on Syria would be seen as a justified humanitarian intervention, less likely to cause civilian casualties than airstrikes, or whether it would only embolden American adversaries who have themselves been debating how to use the new weapons.

Jason Healey, the director of the Cyber Statecraft Initiative at the Atlantic

Council, argues that it is "worth doing to show that cyberoperations are not evil witchcraft but can be humanitarian."

But others caution whether that would really be the perception.

"Here in the U.S. we tend to view a cyberattack as a de-escalation — it's less damaging than airstrikes," said Peter W. Singer, a Brookings Institution scholar and co-author of the recently published book "Cybersecurity and Cyberwar: What Everyone Needs to Know."

"But elsewhere in the world it may well be viewed as opening up a new realm of warfare," he said.

There's little doubt that developing weapons for computer warfare is one of the hottest arenas in defense spending. While the size of the Army and traditional weapons systems are being cut in the Pentagon budget that was released on Monday, cyberweapons and Special Forces are growth areas, though it is difficult to tell precisely how much the government spends.

But Mr. Obama has made no secret of his concerns about using cyberweapons. He narrowed Olympic Games, the program against the Iranian nuclear enrichment program, to make sure that it did not cripple civilian facilities like hospitals.

What he liked about the program was that it was covert and that, if successful, it could help buy time to force the Iranians into negotiations. And that is exactly what happened. But when a technological error in the summer of 2010 resulted in the broadcast of the Stuxnet computer worm around the world, ultimately leading to the revelation of the program's origins with the N.S.A. and Unit 8200 of Israel, Mr. Obama's hopes of keeping such programs at arm's length were dashed.

Since then, there has been no clear evidence that the United States has used the weapons in another major attack. It was considered during the NATO attacks on Libya in the spring of 2011, but dismissed after Mr. Obama's advisers warned him that there was no assurance they would work against Col. Muammar el-Qaddafi's antiquated, pre-Internet air defenses.

The head of the N.S.A., Gen. Keith B. Alexander, said in an interview last year that such weapons had been used only a handful of times in his eight-year tenure.

But Syria is a complicated case, raising different issues than Iran did. In

Syria, the humanitarian impulse to do something, without putting Americans at risk or directly entering the civil war, is growing inside the administration. Most of that discussion focuses on providing more training and arms for what are seen as moderate rebel groups. But cyberweapons are in the conversation about stepping up covert action.

Part of the argument is that Syria is a place where America could change its image, using its most advanced technology for a humanitarian purpose.

"The United States has been caught using Stuxnet to conduct a covert cybercampaign against Iran as well as trawling the Internet with the massive Prism collection operation," Mr. Healey wrote recently, referring to the N.S.A.'s data-mining program. "The world is increasingly seeing U.S. cyberpower as a force for evil in the world. A cyberoperation against Syria might help to reverse this view."

Yet that would require openly taking credit for an attack, something the United States has never done. "The question is whether the president would be willing to give the kind of speech he gave about why it would be justified to shoot off missiles in response to Assad's use of chemical weapons," a senior administration official said. Mr. Obama pulled back from that strike at the last moment.

Even if the United States wanted to act covertly, a cyberattack on Syria would be hard to keep secret. Anything that grounded the air fleet, or turned out the lights at key facilities in Damascus and at major military outposts, would be instantly noticed — and would not necessarily be accomplished quickly.

American military planners concluded after putting together options for Mr. Obama over the past two and a half years that any meaningful attack on Syria's facilities would have to be both long enough to make a difference and targeted enough to keep from making an already suffering population even worse off.

For those and other reasons, there are doubters throughout the military and intelligence establishment. "It would be of limited utility, frankly," one senior administration official said.

For instance, an attack could disrupt or shut down the navigational systems for Syria's aircraft, including the Russian-designed Mi-8 and Mi-17 helicopters that are carrying out many of the so-called barrel-bomb attacks against civilians

in Homs and Aleppo.

But Syrian commanders would probably just shift to other weapons in their arsenal, like an array of rockets and missiles, including longer-range Scud missiles, that Mr. Assad's forces have already employed with deadly effect.

Syria is no stranger to these attacks, either on the receiving or the giving end. A September 2007 strike by Israel that destroyed a nuclear reactor being built in the Syrian desert was accompanied by an ingenious cyberattack that blinded Syria's air defenses. When the Syrian military awoke the next morning, the reactor being built with North Korean help was a smoking hole in the ground, as were some associated facilities.

On the offensive end, the Electronic Frontier Foundation, which follows these issues, assembled evidence in a report published late last year that the Syrians had used a "spear phishing" ploy, which gets the target to click on a link in an email, in this case videos of war atrocities, to identify people who are aiding the rebel groups and get inside their computer systems.

And the Syrian Electronic Army, which American intelligence officials suspect is actually Iranian, has conducted strikes against targets in the United States over the past year, including the website of The New York Times. Mostly these have been denial-of-service attacks, annoying and disruptive, but not truly sophisticated.

The chances that Syria could manage a significant response are low, American officials and outside experts said. But the precedent could embolden the Russians and the Iranians into taking a greater part in a new and escalating form of warfare.

Eric Schmitt contributed reporting.

A version of this article appears in print on February 25, 2014, on page A1 of the New York edition with the headline: Syria War Stirs New U.S. Debate on Cyberattacks.
