The New York Times | http://nyti.ms/1Ls5Lfp

MIDDLE EAST

U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict

By **DAVID E. SANGER** and **MARK MAZZETTI** FEB. 16, 2016

BERLIN — In the early years of the Obama administration, the United States developed an elaborate plan for a cyberattack on Iran in case the diplomatic effort to limit its nuclear program failed and led to a military conflict, according to a coming documentary film and interviews with military and intelligence officials involved in the effort.

The plan, code-named Nitro Zeus, was devised to disable Iran's air defenses, communications systems and crucial parts of its power grid, and was shelved, at least for the foreseeable future, after the nuclear deal struck between Iran and six other nations last summer was fulfilled.

Nitro Zeus was part of an effort to assure President Obama that he had alternatives, short of a full-scale war, if Iran lashed out at the United States or its allies in the region. At its height, officials say, the planning for Nitro Zeus involved thousands of American military and intelligence personnel, spending tens of millions of dollars and placing electronic implants in Iranian computer networks to "prepare the battlefield," in the parlance of the Pentagon.

The United States military develops contingency plans for all kinds of possible conflicts, such as a North Korean attack on the South, loose nuclear weapons in South Asia or uprisings in Africa or Latin America. Most sit on the shelf, and are updated every few years. But this one took on

far greater urgency, in part because White House officials believed there was a good chance that Prime Minister Benjamin Netanyahu of Israel would decide to strike Iran's nuclear facilities, and the United States would be drawn into the hostilities that followed.

While the Pentagon was making those preparations, American intelligence agencies developed a separate, far more narrowly focused cyberplan to disable the Fordo nuclear enrichment site, which Iran built deep inside a mountain near the city of Qum. The attack would have been a covert operation, which the president can authorize even in the absence of a continuing conflict.

Fordo has long been considered one of the hardest targets in Iran, buried too deep for all but the most powerful bunker-buster in the American arsenal. The proposed intelligence operation would have inserted a computer "worm" into the facility with the aim of frying Fordo's computer systems — effectively delaying or destroying the ability of Iranian centrifuges to enrich uranium at the site. It was intended as a follow-up to "Olympic Games," the code name of a cyberattack by the United States and Israel that destroyed 1,000 centrifuges and temporarily disrupted production at Natanz, a far larger but less protected enrichment site.

Under the terms of the nuclear agreement with Iran, two-thirds of the centrifuges inside Fordo have been removed in recent months, along with all nuclear material. The facility is banned from any nuclear-related work and is being converted to other uses, eliminating the threat that prompted the attack plan, at least for the next 15 years.

The development of the two secret programs suggest how seriously the Obama administration was concerned that its negotiations with Iran could fail. It also demonstrates the critical role cyberoperations now play in both military planning and covert intelligence operations. American generals began incorporating nuclear weapons into their war plans for protecting Europe or countering the Soviet Union in the 1950s, and in the last 15 years, they have made armed drones a central part of military efforts in

Pakistan, Afghanistan and elsewhere. In the same way, cyberwarfare has become a standard element of the arsenal for what are now called "hybrid" conflicts.

The existence of Nitro Zeus was uncovered in the course of reporting for "Zero Days," a documentary that will be first shown Wednesday at the Berlin Film Festival. Directed by Alex Gibney, who is known for other documentaries including the Oscar-winning "Taxi to the Dark Side" about the use of torture by American interrogators, and "We Steal Secrets: The Story of WikiLeaks."

"Zero Days" describes the escalating conflict between Iran and the West in the years leading up to the agreement, the discovery of the cyberattack on the Natanz enrichment plant, and the debates inside the Pentagon over whether the United States has a workable doctrine for the use of a new form of weaponry whose ultimate effects are only vaguely understood.

Mr. Gibney and his investigative team, led by Javier Botero, interviewed current and former participants in the Iran program who revealed details of the effort to infuse Iran's computer networks with "implants" that could be used to monitor the country's activities and, if ordered by Mr. Obama, to attack its infrastructure. (Under rules laid out in presidential directives, some made public three years ago by Edward J. Snowden, the former National Security Agency contractor, only the president can authorize an offensive cyberattack, just as the president must approve the use of nuclear weapons.)

The New York Times conducted separate interviews to confirm the outlines of the program. The findings were described over the past two weeks to the White House, the Pentagon, and the Office of the Director of National Intelligence, all of which declined to comment, noting that they never discuss planning for military contingencies.

For the seven-year-old United States Cyber Command, which is still building its cyber "special forces" and deploying them throughout the

world, the Iran project was perhaps its most challenging program yet. “This was an enormous, and enormously complex, program,” said one participant who requested anonymity to discuss a classified program. “Before it was developed, the U.S. had never assembled a combined cyber and kinetic attack plan on this scale.”

Nitro Zeus had its roots in the Bush administration but took on new life in 2009 and 2010, just as Mr. Obama asked General John R. Allen, at United States Central Command, to develop a detailed military plan for Iran in case diplomacy failed. It was a time of extraordinary tension, as the Iranians accelerated their production of centrifuges and produced near-bomb-grade fuel and Western intelligence agencies feared they might be on the verge of developing a nuclear weapon. It was also a period of extraordinary tension with Israel, partly because of its presumed role in the assassination of Iranian nuclear scientists, and partly because of evidence that Mr. Netanyahu was preparing a pre-emptive strike against Iran, despite warnings from the United States.

At the time, Mr. Obama’s aides thought he did not have a credible military contingency plan. In his memoir, “Duty,” former Secretary of Defense Robert M. Gates described his concerns — laid out in a highly restricted memorandum to the White House in January 2010 — that America’s top national security leadership had not even begun to debate what a fast reaction to Iranian aggression would look like.

Nitro Zeus quickly emerged as one possible response for Mr. Obama, a way to turn off critical elements of the Iranian infrastructure without firing a shot. While cyberoperations have long been contemplated in other war scenarios, Nitro Zeus “took it to a new level,” one participant said. Yet the planners warned that depending on how the conflict unfolded, there could be significant effects on civilians, particularly if the United States had to cut vast swaths of the country’s electrical grid and communications networks.

While Cyber Command would have executed Nitro Zeus, the National Security Agency’s Tailored Access Operations unit was responsible for

penetrating adversary networks, which would have required piercing and maintaining a presence in a vast number of Iranian networks, including the country's air defenses and its transportation and command control centers.

It is a tricky business, the war planners say, because their knowledge of how networks are connected in Iran, or any other hard target, is sketchy — and collateral damage is always hard to predict. It is easier to turn off power grids, for example, than to start them up again.

Even as the Pentagon prepared for a broad conflict, American intelligence agencies had a narrower target: how to sabotage the underground Fordo enrichment site, just as they had sabotaged Natanz at the end of the Bush administration and the beginning of the Obama administration.

That effort accelerated in 2012 and 2013, as the Iranians began to fill Fordo's deep underground cavity with more than 3,000 centrifuges. But it was set aside, after the Iranians significantly slowed their enrichment activity during the negotiation over the nuclear deal, and then dismantled part of the Fordo plant.

The program to develop a computer worm to attack Fordo appears to have been initially developed around the time that Mr. Obama and other world leaders revealed the existence of the underground facility at a conference in Pittsburgh in September 2009. It is unclear how American spies planned to get inside the underground nuclear facility — physically or remotely — and whether the United States or an ally like Israel might have had to use human sources inside the country to conduct the network attack.

The Snowden documents revealed a series of technologies that can be used to insert programs remotely in a system disconnected from the Internet. That was done repeatedly at Natanz, as malware was refined and refined again, with each version subtly manipulating the computer controllers for the centrifuges so that the giant, spinning machines would gyrate wildly out of control and destroy themselves. The attack on Fordo appears to have been designed to be more blunt and obvious — a

straightforward strike that would destroy the circuitry that powered the centrifuges and their controllers.

It is unclear how successful the strike would have been. While such efforts are usually tested in mock facilities, there almost certainly would have been surprises had it been used against the Fordo plant. It is also unclear the degree to which American and Israeli intelligence agencies may have collaborated on the program, especially after the recriminations in 2010 over evidence that Israel rushed ahead in producing a version of the Stuxnet worm without properly testing it, leading to its exposure.

David E. Sanger reported from Berlin, and Mark Mazzetti from Washington.

Follow the New York Times's politics and Washington coverage on Facebook and Twitter, and sign up for the First Draft politics newsletter.

A version of this article appears in print on February 17, 2016, on page A5 of the New York edition with the headline: U.S. Drew Up Cyberattack Plan in Case Iran Nuclear Dispute Led to Conflict.
