GlobalResearch
Center for Research on Globalization

“Lights Out!” Did Trump and His Neocons Recycle Bush-Era Plan to Knock Out Venezuela’s Power Grid?

By Whitney Webb
Global Research, March 12, 2019
MintPress News 11 March 2019

Region: Latin America & Caribbean, USA
Theme: History, Law and Justice, Media Disinformation

Even as the Venezuelan government blamed the recent power outage on U.S.-led “sabotage,” the U.S. has long had a plan on the books for targeting the civilian power grid of adversarial nations.

***

For nearly four days, much of Venezuela has been without power, bringing the country’s embattled economy to a near standstill. Though power is now returning, the outage saw U.S. officials and politicians blame the Venezuelan government for the crisis while officials in Caracas accused the U.S. of conducting “sabotage” and launching cyberattacks that targeted its civilian power grid as well as of employing saboteurs within Venezuela.

Although many mainstream media outlets have echoed the official U.S. government response, some journalists have strayed from the pack. One notable example is Kalev Leetaru, who wrote at *Forbes* that “the United States remotely interfering with its [Venezuela’s] power grid is actually quite realistic.”

Leetaru also noted that “timing such an outage to occur at a moment of societal upheaval in a way that delegitimizes the current government, exactly as a government-in-waiting has presented itself as a ready alternative, is actually one of the tactics” he had previously explored in a 2015 article detailing U.S. government hybrid warfare tactics “to weaken an adversary prior to conventional invasion or to forcibly and deniably effect a transition in a foreign government.”

In addition to Leetaru’s claims, others have asserted U.S. government involvement after U.S. Senator Marco Rubio (R-FL), who is deeply involved in Trump’s Venezuela policy, appeared to have prior knowledge that the blackouts would occur when he tweeted about them only three minutes after they had begun.

While several journalists have pointed out that the probability that the Trump administration was responsible for the blackout is highly likely, few — if any — pointed out that the U.S. has long had highly developed plans involving the use of cyberattacks to attack critical power-grid infrastructure in countries targeted for regime change by Washington.

Indeed, the most well-known plan of this type, known by its codename “Nitro Zeus,” was originally created under the George W. Bush administration and was aimed at Iran. With so many former Bush officials now calling the shots in the Trump administration, particularly its

Venezuela policy, the potential return of a "Nitro Zeus" virus, this time tailored to Venezuela, seems increasingly likely.

A little hammer to use when big hammers have been nixed

The "Nitro Zeus" plan first came to light in a November 2016 exposé published in the *New York Times,* which described it as an "elaborate plan" that was created for use against Iran were negotiations over its nuclear program to fail. That program targeted "Iran's air defenses, communications systems and crucial parts of its power grid. At its height it "involved thousands of American military and intelligence personnel" and is believed to have cost tens of millions of dollars. The program intimately involved both the National Security Agency's Tailored Access Operations unit and the U.S. Cyber Command.

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

Screengrab from The New York Times

The program was shelved when the Joint Comprehensive Plan of Action (JCPOA) was established, though the Trump administration's decision to unilaterally withdraw from the deal has led some to ask whether the Trump administration has been considering reviving the program. While they may not have revived it for use against Iran, they instead may have done so in Venezuela, if Venezuelan government assertions that a U.S. cyberattack is to blame for much of the country's recent power outage are to be believed.

Indeed, Leetaru noted in his recent *Forbes* article that "given the U.S. government's longstanding concern with Venezuela's government, it is likely that the U.S. already maintains a deep presence within the country's national infrastructure grid," much as it did with Iran in connection with the Nitro Zeus program prior to its public revelation three years ago.

The Nitro Zeus program is not nearly as well known as its relative, the Stuxnet virus, which was co-developed by the U.S. and Israel and used to attack Iranian software controlling uranium enrichment centers. Yet Nitro Zeus, despite its relative lack of infamy, is notable for several reasons. First, it "took it [U.S. cyberwarfare] to a new level," according to a former official involved in the project cited by the *Times*. This was because, prior to Nitro Zeus, "the U.S. had never assembled a combined cyber and kinetic attack plan on this scale," and also because executing the program would have "significant effects on civilians, particularly if the United States had to cut vast swaths of the country's electrical grid and communications networks."

Another reason Nitro Zeus is notable, particularly in light of U.S. efforts to meddle in Venezuela, is the motive for its creation. Indeed, although Nitro Zeus became the "enormous, and enormously complex" program detailed by the *Times* during the Obama administration, work on the program had actually begun during the George W. Bush administration. According to a report in the *Daily Beast*, Bush had considered Nitro Zeus "a necessary tactical alternative after the Iraq War sabotaged his chances of starting another Middle East invasion." In other words, after the Iraq War debacle made it more difficult for the U.S. to launch unilateral military interventions, the Bush administration opted to develop "non-kinetic" military tools that would avoid angering the U.S. public and U.S. allies abroad.

Furthermore, as Tyler Rogoway wrote at *Foxtrot Alpha*:

> [Programs like Nitro Zeus] can be paired for synergistic effect, leaving its target country's military blind and deaf and its population suffering. And all this can be had without ever dropping a bomb and even under the veil of plausible deniability."

This, according to Rogoway, has led such programs to become "more and more a viable alternative to traditional forms of attack," given that the U.S. can deny its involvement, avoiding potential diplomatic blowback, and because it can wreak havoc not just on a country's military but its civilian population.

The logic behind the likelihood of U.S. cyber sabotage

While "Nitro Zeus" was never unleashed upon Iran, it's likely that the program spawned similar attack plans on the power grids of other adversarial nations given the precedent it set. As the *Times* pointed out in its Nitro Zeus exposé:

> 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."

This point was expanded upon by Rogoway, who noted:

> Nitro Zeus is most likely one of a whole slew of plans to attack potential enemies via cyber weaponry. Plans surely exist for all of America's potential adversaries, and some are likely to be far more elaborate and deadly than anything that has been disclosed to date."

There are more than a few indications that many of the more aggressive "contingency plans" have moved to the top of the toolbox under the Trump administration. For instance, key former Bush officials that are now in the Trump administration, particularly John Bolton and Elliot Abrams, are known for their aggressive stances and willingness to promote extreme policies targeting adversaries, even those policies that harm or kill scores of innocent civilians. Thus, voices like those in the Obama State Department and National Security Council, who had warned of the potential adverse effects on civilians that a Nitro Zeus blackout could cause, are unlikely to influence the likes of Bolton and Abrams — who have an outsized role in creating the administration's Venezuela policy.

Furthermore, such a plan would be considered valuable by Bolton and Abrams in the same way that Bush valued Nitro Zeus after his "hands were tied" following the Iraq War disaster. In regard to Venezuela, Bolton and Abrams similarly have their hands tied when it comes to military action, given that military intervention of any type has been resoundingly rejected by the U.S.' allies in Latin America and elsewhere. Not only that but Abrams' favored tactic of providing arms disguised as "humanitarian aid" to insurgents has also failed, limiting the aggressive actions that can be taken by the administration.

Unable to launch a military intervention — either overt or covert — a Nitro Zeus cyberattack would likely have been a top contender for a next step following the failed "humanitarian aid" stunt and the rejection of any type of military intervention by the U.S.' Latin American allies.

In addition, many of those responsible for the creation of the Nitro Zeus program share connections with neoconservatives who are influential in the Trump administration. For instance, Keith Alexander — who was NSA director at the time the Nitro Zeus program began and for much of its development — is now the CEO of his new cybersecurity consultancy, IronNet Cybersecurity. Sitting on IronNet's board of directors alongside Alexander is Jack Keane, a zealously pro-war retired general whom Trump valued enough to offer the position of Secretary of Defense, an offer Keane declined. Keane is a close associate of the neoconservative Kagan family and is currently chairman of the Institute for the Study of War, founded by Kimberly Kagan and financed by top U.S. weapons companies.

With Bush-era warmongers now dominating Trump's Venezuela policy, it seems increasingly likely that efforts to revive the Bush/Obama-era Nitro Zeus program have taken place. Indeed, with such an enormous and complex program already on the books and the likely existence of spin-off programs that have developed over the past decade, it was likely the easiest route for another "aggressive" U.S.-backed measure targeting the Venezuelan government.

However, if the U.S. did conduct a cyber attack on Venezuela's power grid, it would not be powerful neoconservatives in the administration who would ultimately be to blame, as only the U.S. president can authorize an offensive cyberattack. Thus, if any part of Venezuela's current blackout was indeed U.S.-directed sabotage, it was President Donald Trump who gave the order to attack Venezuela's civilian power infrastructure, a strange thing to do for someone who professes to care so much for the Venezuelan people.

*

Note to readers: please click the share buttons below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Whitney Webb is a MintPress News journalist based in Chile. She has contributed to several independent media outlets including Global Research, EcoWatch, the Ron Paul Institute and 21st Century Wire, among others. She has made several radio and television appearances and is the 2019 winner of the Serena Shim Award for Uncompromised Integrity in Journalism.

Featured image is from Axios
