GlobalResearch
Center for Research on Globalization

Trump Regime Electricity War in Venezuela More Serious than First Believed

By Stephen Lendman
Global Research, March 11, 2019

Region: Latin America & Caribbean
Theme: US NATO War Agenda

On Thursday, Venezuela's Guri dam hydroelectric power plant was cyberattacked at 5:00 PM during the late afternoon rush hour to cause maximum disruption.

Up to 80% of the country was affected, damage done more severe than initially thought. Weeks or months of planning likely preceded what happened – US behind it? considerable expertise needed to pull it off.

On Friday, another cyberattack occurred, followed by a third one on Saturday, affecting parts of the country where power was restored, further complicating resolution of the problem, Maduro saying:

After power was restored to about 70% of the country, "we received another attack, of a cybernetic nature, at midday…that disturbed the reconnection process and knocked out everything that had been achieved until noon," adding:

> "(O)ne of the sources of generation that was working perfectly" was sabotaged again…infiltrators…attacking the electric company from the inside."

Power is being restored "manually," efforts continuing to learn precisely why computerized systems failed – things further complicated after a Bolivar state substation transformer exploded and burned, suggesting more sabotage.

What's happening in Venezuela is similar to infecting Iran's Bushehr and Natanz nuclear power facilities with a Stuxnet malware computer virus in 2010, a likely joint US/Israeli intelligence operation. Edward Snowden blamed them for what happened.

At the time, operations were halted indefinitely. Iran called the incident a hostile act. General Gholam-Reza Jalali said if the affected facilities went online infected, Iran's entire electrical power grid could have been shut down.

It took months to fully resolve the problem. Following the summer 2010 attack, the malware continued to infect the facilities' centrifuges, requiring their replacement.

An Institute for Science and International Security analysis said

> "(a)ssuming Iran exercises caution, Stuxnet is unlikely to destroy more centrifuges at the (affected plants)."
>
> "Iran likely cleaned the malware from its control systems. To prevent re-

> infection, Iran will have to exercise special caution since so many computers in Iran contain Stuxnet," adding:
>
> "Although Stuxnet appears to be designed to destroy centrifuges at (Iranian nuclear facilities), destruction was by no means total."
>
> "Stuxnet did not lower the production of low-enriched uranium (LEU) during 2010. LEU quantities could have certainly been greater, and Stuxnet could be an important part of the reason why they did not increase significantly."
>
> "(T)here remain important questions about why Stuxnet destroyed only 1,000 centrifuges. One observation is that it may be harder to destroy centrifuges by use of cyber attacks than often believed."

Head of Bushehr's nuclear power plant said only personal computers of staff were infected by the Stuxnet virus. Then-Iranian Telecommunications Minister Reza Taghipour said government systems experienced no serious damage.

Iran's Information Technology Council director Mahmud Liaii said

> "(a)n electronic war has been launched against Iran... This computer worm is designed to transfer data about production lines from our industrial plants to locations outside Iran."

Deputy head of Iran's government Information Technology Company Hamid Alipour said

> "(t)he attack is still ongoing and new versions of this virus are spreading," adding:
>
> "We had anticipated that we could root out the virus within one to two months, but the virus is not stable, and since we started the cleanup process three new versions of it have been spreading."

If malware similar to Stuxnet was used against Venezuela's power grid, the problem could linger for months, parts of the country continued to be affected by outages for some time.

Maduro's government will need to marshal considerable technical expertise to fully resolve things – the type cybersecurity/anti-virus/security software skills Russia-based multinational firm Kaspersky Lab can provide.

It can also identify the attack's source and lay blame where it belongs – the US most likely responsible. It clearly has motive, opportunity and expertise – waging war on Venezuela by other means to topple its government and gain another imperial trophy.

If the malware infection is widespread, continued outages may happen until the problem is fully resolved.

Resolution may take months, disruption in the country persisting, clearly the motive behind the attack.

*

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

Award-winning author Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. He is a Research Associate of the Centre for Research on Globalization (CRG)

His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III."

http://www.claritypress.com/LendmanIII.html

Visit his blog site at sjlendman.blogspot.com.

Featured image is from Novinite.com

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Stephen Lendman

About the author:

Stephen Lendman lives in Chicago. He can be reached at lendmanstephen@sbcglobal.net. His new book as editor and contributor is titled "Flashpoint in Ukraine: US Drive for Hegemony Risks WW III." http://www.claritypress.com/LendmanIII.html Visit his blog site at sjlendman.blogspot.com. Listen to cutting-edge discussions with distinguished guests on the Progressive Radio News Hour on the Progressive Radio Network. It airs three times weekly: live on Sundays at 1PM Central time plus two prerecorded archived programs.