

Fake News? Russia Attacks Vermont? Penetrated the Electric Grid.

By [Stephen Lendman](#)

Global Research, January 01, 2017

Region: [Russia and FSU](#), [USA](#)

Theme: [Intelligence](#), [Media Disinformation](#)

Sound absurd? It is, part of intense Russia bashing, a political and economic assault, risking something more serious.

On New Year's eve, the [Washington Post](#) published an updated version of its previous fake news story.

The earlier version claimed Russian hackers penetrated the US electric grid – a Big Lie. The new version says it hacked a Vermont utility, citing the usual unnamed US sources.

WaPo: “(T)he discovery underscores the vulnerabilities of the nation’s electrical grid. And it raises fears in the US government that Russian government hackers are actively trying to penetrate the grid to carry out potential attacks.”

Fact: As usual, when it comes to bashing Russia, claims aren’t backed by verifiable evidence, just fear-mongering hyperbole – media repeating it without due diligence checking for veracity.

Russia poses no threat to any country – not to America, its electricity grid, Vermont or any other state, city or federal operation.

Claiming it was fake news like all other anti-Russia accusations, not a shred of evidence supporting them.

Claiming “(a) code associated with the Russian hacking operation dubbed Grizzly Steppe by the Obama administration has been detected within the system of a Vermont utility” was willful deception.

Cybersecurity specialists said the code wasn’t Russian. It was an outdated Ukrainian hacking tool. On Friday, Burlington Electric said the malware code was detected during a single laptop scan not connected to its power grid.

A company statement said “(w)e took immediate action to isolate the laptop and alerted federal officials of this finding.”

Our team is working with federal officials to trace this malware and prevent any other attempts to infiltrate utility systems. We have briefed state officials and will support the investigation fully.

Blaming Russia for hyped incidents is the usual knee-jerk response, part of longstanding

bashing, ongoing now to pressure Trump against normalizing ties, including cooperating with Putin in combating terrorism.

A report on the Vermont incident by cybersecurity firm [Wordfence](#) said alleged originating IP addresses provided by US agencies “don’t appear to provide any association with Russia.” They’re “probably used by a wide range of other malicious actors.”

Vermonters can relax. So can Americans in the other 49 states. The Russians aren’t coming. No Russian cyber or other attacks loom.

Claims otherwise are fabricated for political reasons – not legitimate ones.

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: How the 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.

The original source of this article is Global Research
Copyright © [Stephen Lendman](#), Global Research, 2017

[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.

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca