

Russia Hysteria Infects WashPost Again: False Story About Hacking U.S. Electric Grid

By [Glenn Greenwald](#)


Global Research, January 03, 2017

[TheIntercept](#) 31 December 2016

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

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

The Washington Post on Friday reported a [genuinely alarming event](#): Russian hackers have penetrated the U.S. power system through an electrical grid in Vermont. The Post headline conveyed the seriousness of the threat.

The first sentence of the article directly linked this cyberattack to alleged Russian hacking of the email accounts of the DNC and John Podesta — what is now routinely referred to as “Russian hacking of our election” — by referencing the code name revealed on Wednesday by the Obama administration when it announced sanctions on Russian officials: “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, according to U.S. officials.”

The Post article contained grave statements from Vermont officials of the type politicians love to issue after a terrorist attack to show they are tough and in control. The state’s Democratic governor, Peter Shumlin, said:

Vermonters and all Americans should be both alarmed and outraged that one of the world’s leading thugs, Vladimir Putin, has been attempting to hack our electric grid, which we rely upon to support our quality of life, economy, health, and safety. This episode should highlight the urgent need for our federal government to vigorously pursue and put an end to this sort of Russian meddling.

Vermont Sen. Patrick Leahy [issued a statement](#) warning: “This is beyond hackers having electronic joy rides — this is now about trying to access utilities to potentially manipulate the grid and shut it down in the middle of winter. That is a direct threat to Vermont and we do not take it lightly.”

The article went on and on in that vein, with all the standard tactics used by the U.S. media for such stories: quoting anonymous national security officials, reviewing past acts of Russian treachery, and drawing the scariest possible conclusions (“The question remains: Are they in other systems and what was the intent?” a U.S. official said”).

The media reactions, as [Alex Pfeiffer documents](#), were exactly what one would expect: hysterical, alarmist proclamations of Putin’s menacing evil:

Our Russian “friend” Putin attacked the U.S. power grid.<https://t.co/iAneRgbuhF>

— Brent Staples (@BrentNYT) [December 31, 2016](#)

NEW: “One of the world’s leading thugs, [Putin] has been attempting to hack our electric grid,” says VT Gov. Shumlin <https://t.co/YgdtT4JrlXpic.twitter.com/AU0ZQjT3aO>

— ABC News (@ABC) [31 December 2016](#)

Yikes. <https://t.co/cXsyd1RHOK>

— Paul Farhi (@farhip) [31 December 2016](#)

The Post’s story also predictably and very rapidly infected other large media outlets. Reuters [thus told its readers](#) around the world: “A malware code associated with Russian hackers has reportedly been detected within the system of a Vermont electric utility.”

WHAT’S THE PROBLEM here? It did not happen.

There was no “penetration of the U.S. electricity grid.” The truth was undramatic and banal. Burlington Electric, after receiving a Homeland Security notice sent to all U.S. utility companies about the malware code found in the DNC system, searched all its computers and found the code in a single laptop that *was not connected to the electric grid*.

Apparently, the Post did not even bother to contact the company before running its wildly sensationalistic claims, so Burlington Electric had to [issue its own statement to the Burlington Free Press](#), which debunked the Post’s central claim (emphasis in original): “We detected the malware in a single Burlington Electric Department laptop NOT connected to our organization’s grid systems.”

So the key scary claim of the Post story — that Russian hackers had penetrated the U.S. electric grid — was false. All the alarmist tough-guy statements issued by political officials who believed the Post’s claim were based on fiction.

Even worse, there is zero evidence that Russian hackers were even responsible for the implanting of this malware on this single laptop. The fact that malware is “Russian-made” does not mean that only Russians can use it; indeed, like a lot of malware, it can be purchased (as Jeffrey Carr has [pointed out in the DNC hacking context](#), assuming that Russian-made malware must have been used by Russians is as irrational as finding a Russian-made Kalashnikov AKM rifle at a crime scene and assuming the killer must be Russian).

As the actual truth emerged once the utility company issued its statement, the Post rushed to fix its embarrassment, beginning by dramatically changing its headline:



The headline is still absurd: They have no idea that this malware was placed by a “Russian operation” (though they would likely justify that by pointing out that they are just stenographically passing along what “officials say”). Moreover, nobody knows when this malware was put on this laptop, how, or by whom. But whatever else is true, the key claim — “Russian hackers penetrated U.S. electricity grid” — has now been replaced by the claim that this all shows “risk to U.S. electrical grid.”

As journalists realized what did — and did not — actually happen here, the reaction was swift:

- 1) Not an infiltration of the power grid.
- 2) “Russian” malware can be purchased online by anyone.
- 3) See 1 & 2. <https://t.co/bVIG8zQBsk>

— Dell Cameron (@dellcam) [31 December 2016](#)

Statement from the Burlington utility, per that BFP story.
pic.twitter.com/25cHENWh0a

— Eric Geller (@ericgeller) [31 December 2016](#)

My money's on this all turns out to be commodity malware and not even APT28/APT29 and everyone jumping on the bandwagon will look v silly

— Pwn All The Things (@pwnallthethings) [31 December 2016](#)

This matters not only because one of the nation's major newspapers [once again](#) published a wildly misleading, fearmongering story about Russia. It matters even more because it reflects the deeply irrational and ever-spiraling fever that is being cultivated in U.S. political discourse and culture about the threat posed by Moscow.

The Post has many excellent reporters and smart editors. They have produced [many great stories this year](#). But this kind of blatantly irresponsible and sensationalist tabloid behavior — which tracks what they did when [promoting that grotesque PropOrNot blacklist](#) of U.S. news outlets accused of being Kremlin tools — is a byproduct of the Anything Goes mentality that now shapes mainstream discussion of Russia, Putin, and the Grave Threat to All Things Decent in America that they pose.

The level of groupthink, fearmongering, coercive peer pressure, and über-nationalism has not been seen since the halcyon days of 2002 and 2003. Indeed, the [very same people](#) who back then smeared [anyone questioning official claims](#) as Saddam sympathizers or stooges and left-wing un-American loons are [back for their sequel](#), accusing anyone who expresses any skepticism toward claims about Russia of being Putin sympathizers and Kremlin operatives and stooges.

But it's all severely exacerbated by social media in ways that we don't yet fully understand. A large percentage of journalists sit on Twitter all day. It's their primary window into the world. Because of how intense and raw the emotions still are from Trump's defeat of Clinton, the social media benefits from tweeting and publishing unhinged claims about Trump and Putin are immense and immediate: thousands upon thousands of re-tweets, a rapidly building follower count, and huge amounts of traffic.

Indeed, the more unhinged it is, the greater the benefits are (see some of the [most extreme](#)

[examples here](#)). That's how otherwise rational people [keep getting tricked](#) into posting and re-tweeting and sharing extremely dubious stories [that turn out to be false](#).

And that's to say nothing of the non-utilitarian social pressures. It's not news that coastal elites — particularly media and political figures — were and are virtually unified in their unbridled contempt for Trump. And we have seen over and over that any time there is a new Prime Foreign Villain consecrated — now Putin — U.S. media figures lead the campaign. As a result, any denunciation or accusation toward Trump or Russia, no matter how divorced from reason or devoid of facts, generates instant praise, while any questioning of it prompts instant peer-group denunciation, or worse.

Few things are more dangerous to the journalistic function than groupthink, and few instruments have been invented that foster and reinforce groupthink like social media, particularly Twitter, the platform most used by journalists. That's a phenomenon that merits far more study, but examples like this one highlight the dynamic.

In this case, the effect is a constant ratcheting up of tensions [between two nuclear-armed powers](#) whose nuclear systems are still on hair-trigger alert and capable of catastrophic responses based on misunderstanding and misperception. Democrats and their media allies are rightly alarmed about the potential dangers of Trump's bellicose posture toward China, but remarkably and recklessly indifferent to the dangers of what they themselves are doing here.

* * * * *

Those interested in a sober and rational discussion of the Russia hacking issue should read the following:

(1) Three posts by cybersecurity expert Jeffrey Carr: first, on the [difficulty of proving attribution for any hacks](#); second, [on the irrational claims](#) on which the "Russia hacked the DNC" case is predicated; and third, on the [woefully inadequate, evidence-free report](#) issued by the Department of Homeland Security and FBI this week to justify sanctions against Russia.

(2) Yesterday's [Rolling Stone article by Matt Taibbi](#), who lived and worked for more than a decade in Russia, titled: "Something About This Russia Story Stinks."

(3) An [Atlantic article by David A. Graham](#) on the politics and strategies of the sanctions imposed this week on Russia by Obama; I disagree with several of his claims, but the article is a rarity: a calm, sober, rational assessment of this debate.

Since it is so often distorted, permit me once again to underscore my own view on the broader Russia issue: Of course it is possible that Russia is responsible for these hacks, as this is perfectly consistent with (and far more mild than) what both Russia and the U.S. have done repeatedly for decades.

But given the stakes involved, along with the incentives for error and/or deceit, no rational person should be willing to embrace these accusations as Truth unless and until convincing evidence has been publicly presented for review, which most certainly [has not](#) yet [happened](#). As the above articles demonstrate, this week's proffered "evidence" — the U.S. government's evidence-free report — should raise rather than dilute suspicions. It's hard to understand how this desire for convincing evidence before acceptance of official

claims could even be controversial, particularly among journalists.

UPDATE: Just as [The Guardian had to do just two days ago](#) regarding its claim about WikiLeaks and Putin, the Washington Post has now added an editor's note to its story acknowledging that its key claim was false:



Is it not very clear that journalistic standards are being casually dispensed with when the subject is Russia?

The original source of this article is [TheIntercept](#)
Copyright © [Glenn Greenwald](#), [TheIntercept](#), 2017

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Glenn Greenwald](#)

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