Mainstream Media’s Russian Bogeymen

Exclusive: The mainstream hysteria over Russia has led to dubious or downright false stories that have deepened the New Cold War, as Gareth Porter notes regarding last month’s bogus tale of a hack into the U.S. electric grid.

By Gareth Porter

In the middle of a major domestic crisis over the U.S. charge that Russia had interfered with the U.S. election, the Department of Homeland Security (DHS) triggered a brief national media hysteria by creating and spreading a bogus story of Russian hacking into U.S. power infrastructure.

DHS had initiated the now-discredited tale of a hacked computer at the Burlington, Vermont Electricity Department by sending the utility’s managers misleading and alarming information, then leaked a story they certainly knew to be false and continued to put out a misleading line to the media.

Even more shocking, however, DHS had previously circulated a similar bogus story of Russian hacking of a Springfield, Illinois water pump in November 2011.

The story of how DHS twice circulated false stories of Russian efforts to sabotage U.S. “critical infrastructure” is a cautionary tale of how senior leaders in a bureaucracy-on-the-make take advantage of every major political development to advance its own interests, with scant regard for the truth.

The DHS had carried out a major public campaign to focus on an alleged Russian threat to U.S. power infrastructure in early 2016. The campaign took advantage of a U.S. accusation of a Russian cyber-attack against the Ukrainian power infrastructure in December 2015 to promote one of the agency’s major functions – guarding against cyber-attacks on America’s infrastructure.

Beginning in late March 2016, DHS and FBI conducted a series of 12 unclassified briefings for electric power infrastructure companies in eight cities titled, “Ukraine Cyber Attack: implications for U.S. stakeholders.” The DHS declared publicly, “These events represent one of the first known physical impacts to critical infrastructure which resulted from cyber-attack.”

That statement conveniently avoided mentioning that the first cases of such destruction of national infrastructure from cyber-attacks were not against the United States, but were inflicted on Iran by the Obama administration and Israel in 2009 and 2012.

Beginning in October 2016, the DHS emerged as one of the two most important

players – along with the CIA—in the political drama over the alleged Russian effort to tilt the 2016 election toward Donald Trump. Then on Dec. 29, DHS and FBI distributed a "Joint Analysis Report" to U.S. power utilities across the country with what it claimed were "indicators" of a Russian intelligence effort to penetrate and compromise U.S. computer networks, including networks related to the presidential election, that it called "GRIZZLY STEPPE."

The report clearly conveyed to the utilities that the "tools and infrastructure" it said had been used by Russian intelligence agencies to affect the election were a direct threat to them as well. However, according to Robert M. Lee, the founder and CEO of the cyber-security company Dragos, who had developed one of the earliest U.S. government programs for defense against cyber-attacks on U.S. infrastructure systems, the report was certain to mislead the recipients.

"Anyone who uses it would think they were being impacted by Russian operations," said Lee. "We ran through the indicators in the report and found that a high percentage were false positives."

Lee and his staff found only two of a long list of malware files that could be linked to Russian hackers without more specific data about timing. Similarly a large proportion of IP addresses listed could be linked to "GRIZZLY STEPPE" only for certain specific dates, which were not provided.

The Intercept discovered, in fact, that 42 percent of the 876 IP addresses listed in the report as having been used by Russian hackers were exit nodes for the Tor Project, a system that allows bloggers, journalists and others – including some military entities – to keep their Internet communications private.

Lee said the DHS staff that worked on the technical information in the report is highly competent, but the document was rendered useless when officials classified and deleted some key parts of the report and added other material that shouldn't have been in it. He believes the DHS issued the report "for a political purpose," which was to "show that the DHS is protecting you."

Planting the Story, Keeping it Alive

Upon receiving the DHS-FBI report the Burlington Electric Company network security team immediately ran searches of its computer logs using the lists of IP addresses it had been provided. When one of IP addresses cited in the report as an indicator of Russian hacking was found on the logs, the utility immediately called DHS to inform it as it had been instructed to do by DHS.

In fact, the IP address on the Burlington Electric Company's computer was simply the Yahoo e-mail server, according to Lee, so it could not have been a

legitimate indicator of an attempted cyber-intrusion. That should have been the end of the story. But the utility did not track down the IP address before reporting it to DHS. It did, however, expect DHS to treat the matter confidentially until it had thoroughly investigated and resolved the issue.

“DHS wasn’t supposed to release the details,” said Lee. “Everybody was supposed to keep their mouth shut.”

Instead, a DHS official called The Washington Post and passed on word that one of the indicators of Russian hacking of the DNC had been found on the Burlington utility’s computer network. The Post failed to follow the most basic rule of journalism, relying on its DHS source instead of checking with the Burlington Electric Department first. The result was the Post’s sensational Dec. 30 story under the headline “Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say.”

DHS official evidently had allowed the Post to infer that the Russians hack had penetrated the grid without actually saying so. The Post story said the Russians “had not actively used the code to disrupt operations of the utility, according to officials who spoke on condition of anonymity in order to discuss a security matter,” but then added, and that “the penetration of the nation’s electrical grid is significant because it represents a potentially serious vulnerability.”

The electric company quickly issued a firm denial that the computer in question was connected to the power grid. The Post was forced to retract, in effect, its claim that the electricity grid had been hacked by the Russians. But it stuck by its story that the utility had been the victim of a Russian hack for another three days before admitting that no such evidence of a hack existed.

The day after the story was published, the DHS leadership continued to imply, without saying so explicitly, that the Burlington utility had been hacked by Russians. Assistant Secretary for Pubic Affairs J. Todd Breasseale gave CNN a statement that the “indicators” from the malicious software found on the computer at Burlington Electric were a “match” for those on the DNC computers.

As soon as DHS checked the IP address, however, it knew that it was a Yahoo cloud server and therefore not an indicator that the same team that allegedly hacked the DNC had gotten into the Burlington utility’s laptop. DHS also learned from the utility that the laptop in question had been infected by malware called “neutrino,” which had never been used in “GRIZZLY STEPPE.”

Only days later did the DHS reveal those crucial facts to the Post. And the DHS was still defending its joint report to the Post, according to Lee, who got part of the story from Post sources. The DHS official was arguing that it had “led to

a discovery," he said. "The second is, 'See, this is encouraging people to run indicators.'"

Original DHS False Hacking Story

The false Burlington Electric hack scare is reminiscent of an earlier story of Russian hacking of a utility for which the DHS was responsible as well. In November 2011, it reported an "intrusion" into a Springfield, Illinois water district computer that similarly turned out to be a fabrication.

Like the Burlington fiasco, the false report was preceded by a DHS claim that U.S. infrastructure systems were already under attack. In October 2011, acting DHS deputy undersecretary Greg Schaffer was quoted by The Washington Post as warning that "our adversaries" are "knocking on the doors of these systems." And Schaffer added, "In some cases, there have been intrusions." He did not specify when, where or by whom, and no such prior intrusions have ever been documented.

On Nov. 8, 2011, a water pump belonging to the Curran-Gardner township water district near Springfield, Illinois, burned out after sputtering several times in previous months. The repair team brought in to fix it found a Russian IP address on its log from five months earlier. That IP address was actually from a cell phone call from the contractor who had set up the control system for the pump and who was vacationing in Russia with his family, so his name was in the log by the address.

Without investigating the IP address itself, the utility reported the IP address and the breakdown of the water pump to the Environmental Protection Agency, which in turn passed it on to the Illinois Statewide Terrorism and Intelligence Center, also called a fusion center composed of Illinois State Police and representatives from the FBI, DHS and other government agencies.

On Nov. 10 – just two days after the initial report to EPA – the fusion center produced a report titled "Public Water District Cyber Intrusion" suggesting a Russian hacker had stolen the identity of someone authorized to use the computer and had hacked into the control system causing the water pump to fail.

The contractor whose name was on the log next to the IP address later told Wired magazine that one phone call to him would have laid the matter to rest. But the DHS, which was the lead in putting the report out, had not bothered to make even that one obvious phone call before opining that it must have been a Russian hack.

The fusion center "intelligence report," circulated by DHS Office of Intelligence and Research, was picked up by a cyber-security blogger, who called The Washington Post and read the item to a reporter. Thus the Post published the

first sensational story of a Russian hack into a U.S. infrastructure on Nov. 18, 2011.

After the real story came out, DHS disclaimed responsibility for the report, saying that it was the fusion center's responsibility. But a Senate subcommittee investigation revealed in a report a year later that even after the initial report had been discredited, DHS had not issued any retraction or correction to the report, nor had it notified the recipients about the truth.

DHS officials responsible for the false report told Senate investigators such reports weren't intended to be "finished intelligence," implying that the bar for accuracy of the information didn't have to be very high. They even claimed that report was a "success" because it had done what "what it's supposed to do – generate interest."

Both the Burlington and Curran-Gardner episodes underline a central reality of the political game of national security in the New Cold War era: major bureaucratic players like DHS have a huge political stake in public perceptions of a Russian threat, and whenever the opportunity arises to do so, they will exploit it.

Gareth Porter is an independent investigative journalist and winner of the 2012 Gellhorn Prize for journalism. He is the author of the newly published *Manufactured Crisis: The Untold Story of the Iran Nuclear Scare.*