Fresh Doubts about Russian ‘Hacking’

Exclusive: The gauzy allegations of Russia “hacking” the Democrats to elect Donald Trump just got hazier with WikiLeaks’ new revelations about CIA cyber-spying and the capability to pin the blame on others, reports Robert Parry.

By Robert Parry

WikiLeaks’ disclosure of documents revealing CIA cyber-spying capabilities underscores why much more skepticism should have been applied to the U.S. intelligence community’s allegations about Russia “hacking” last year’s American presidential election. It turns out that the CIA maintains a library of foreign malware that could be used to pin the blame for a “hack” on another intelligence service.

That revelation emerged from documents that WikiLeaks published on Tuesday from a CIA archive that WikiLeaks said had apparently been passed around within a community of former U.S. government hackers and contractors before one of them gave WikiLeaks some of the material.

The documents revealed that the CIA can capture the content of encrypted Internet and cell-phone messages by grabbing the material in the fraction of a second before the words are put through encryption.

Another program called “Weeping Angel” can hack Samsung “smart” TVs with built-in Internet connections, allowing the CIA and British intelligence to covertly use the TVs as listening devices even when they appear to be turned off.

Besides the *1984*-ish aspects of these reported capabilities – Orwell’s dystopia also envisioned TVs being used to spy on people in their homes – the WikiLeaks’ disclosures add a new layer of mystery to whether the Russians were behind the “hacks” of the Democratic Party or whether Moscow was framed.

For instance, the widely cited Russian fingerprints on the “hacking” attacks – such as malware associated with the suspected Russian cyber-attackers APT 28 (also known as “Fancy Bear”); some Cyrillic letters: and the phrase “Felix Edmundovich,” a reference to Dzerzhinsky, the founder of a Bolsheviks’ secret police – look less like proof of Russian guilt than they did earlier.

Or put differently – based on the newly available CIA material – the possibility that these telltale signs were planted to incriminate Moscow doesn’t sound as farfetched as it might have earlier.

A former U.S. intelligence officer, cited by The Wall Street Journal on

Wednesday, acknowledged that the CIA's "Umbrage" library of foreign hacking tools could "be used to mask a U.S. operation and make it appear that it was carried out by another country…. That could be accomplished by inserting malware components from, say, a known Chinese, Russian or Iranian hacking operation into a U.S. one."

While that possibility in no way clears Moscow in the case of the Democratic "hack," it does inject new uncertainty into the "high confidence" that President Obama's intelligence community expressed in its assessment of Russian culpability. If the CIA had this capability to plant false leads in the data, so too would other actors, both government and private, to cover their own tracks.

Dubious Forensics

Another problem with the U.S. intelligence community's assessment is that the forensics were left to private contractors working for the Democrats, not conducted independently by U.S. government experts.

That gap in the evidentiary trail widens when one notes that CrowdStrike, the Democratic Party's consultant, offered contradictory commentary about the skills of the hackers.

CrowdStrike praised the hackers' tradecraft as "superb, operational security second to none" and added: "we identified advanced methods consistent with nation-state level capabilities including deliberate targeting and 'access management' tradecraft – both groups were constantly going back into the environment to change out their implants, modify persistent methods, move to new Command & Control channels and perform other tasks to try to stay ahead of being detected."

In other words, CrowdStrike cited the sophistication of the tradecraft as proof of a state-sponsored cyber-attack, yet it was the sloppiness of the tradecraft that supposedly revealed the Russian links, i.e. the old malware connections, the Cyrillic letters and the Dzerzhinsky reference.

As Sam Biddle wrote for The Intercept, "Would a group whose 'tradecraft is superb' with 'operational security second to none' really leave behind the name of a Soviet spy chief imprinted on a document it sent to American journalists? Would these groups really be dumb enough to leave cyrillic comments on these documents? Would these groups that 'constantly [go] back into the environment to change out their implants, modify persistent methods, move to new Command & Control channels' get caught because they precisely *didn't* make sure not to use IP addresses they'd been associated [with] before?

"It's very hard to buy the argument that the Democrats were hacked by one of the

most sophisticated, diabolical foreign intelligence services in history, and that we know this because they screwed up over and over again."

Sources and Methods

The WikiLeaks' disclosures on Tuesday also demonstrate that the pro-transparency Web site has a well-placed source with access to sensitive U.S. intelligence data.

That reinforces the suggestion from WikiLeaks' associate, former British Ambassador Craig Murray, that the emails purloined from Hillary Clinton's campaign chairman John Podesta originated from U.S. intelligence intercepts and were then leaked by an American insider to WikiLeaks, not obtained via a "hack" directed by the Russian government.

Podesta's association with the international lobbying firm, the Podesta Group, could justify U.S. intelligence monitoring his communications as a way to glean information about the strategies of Saudi Arabia and other foreign clients.

Murray suggested that the earlier WikiLeaks' release of Democratic National Committee emails came from a Democratic insider, not from Russia. In addition, WikiLeaks' founder Julian Assange has denied that Russia was the source of either batch of Democratic emails, although he refused to say who was.

Of course, it would be possible that Russia used American cutouts to launder the emails without WikiLeaks knowing where the material originated. And some cyber-experts, who were cited in press reports about the new WikiLeaks' disclosures on Tuesday, speculated, without evidence, that perhaps Russia was the source of them, too.

Still, there are now fresh reasons to doubt the Official Narrative that Russia "hacked" into Democratic emails in a covert operation intended to throw the U.S. election to Donald Trump.

Those doubts already existed – or should have – because the U.S. intelligence community refused to release any hard proof that the Russians were responsible for the purloined Democratic emails.

On Jan. 6, just one day after Director of National Intelligence James Clapper vowed to go to the greatest possible lengths to supply the public with the evidence behind the accusations, his office released a 25-page report that contained no direct evidence that Russia delivered hacked emails from the DNC and Podesta to WikiLeaks.

The DNI report amounted to a compendium of reasons to suspect that Russia was

the source of the information – built largely on the argument that Russia had a motive for doing so because of its disdain for Democratic nominee Clinton and the potential for friendlier relations with Republican nominee Trump.

A Big Risk

But the DNI's case, as presented, was one-sided, ignoring other reasons why the Russians would not have taken the risk.

For instance, while it is true that many Russian officials, including President Putin, considered Clinton to be a threat to worsen the already frayed relationship between the two nuclear superpowers, the report ignores the downside for Russia trying to interfere with the U.S. election campaign and then failing to stop Clinton, which looked like the most likely outcome until Election Night.

If Russia had accessed the DNC and Podesta emails and slipped them to WikiLeaks for publication, Putin would have to think that the National Security Agency, with its exceptional ability to track electronic communications around the world, might well have detected the maneuver and would have informed Clinton.

So, on top of Clinton's well-known hawkishness, Putin would have risked handing the expected incoming president a personal reason to take revenge on him and his country. Historically, Russia has been very careful in such situations, holding its intelligence collections for internal purposes only and not sharing them with the public.

While it is conceivable that Putin decided to take this extraordinary risk in this case – despite the widely held view that Clinton was a shoo-in to defeat Trump – an objective report would have examined this counter argument for him not doing so.

But the DNI report was not driven by a desire to be evenhanded; it was, in effect, a prosecutor's brief, albeit one that lacked any real evidence that the accused is guilty.

Though it's impossible for an average U.S. citizen to know precisely what the U.S. intelligence community may have in its secret files, some former NSA officials who are familiar with the agency's eavesdropping capabilities say Washington's lack of certainty suggests that the NSA does not possess such evidence.

That's the view of William Binney, who retired as NSA's technical director of world military and geopolitical analysis and who created many of the collection systems still used by NSA.

Binney, in an article co-written with former CIA analyst Ray McGovern, said, "With respect to the alleged interference by Russia and WikiLeaks in the U.S. election, it is a major mystery why U.S. intelligence feels it must rely on 'circumstantial evidence,' when it has NSA's vacuum cleaner sucking up hard evidence galore. What we know of NSA's capabilities shows that the email disclosures were from leaking, not hacking."

Released last summer – around the time of the Democratic National Convention – the DNC emails revealed senior party officials showing a preference for former Secretary of State Clinton over Sen. Bernie Sanders although the DNC was supposed to remain neutral.

Later in the campaign, the Podesta leak exposed the contents of speeches that Clinton gave to Wall Street banks, which she wanted to keep secret from the American voters, and the existence of pay-to-play features of the Clinton Foundation.

News articles based on the WikiLeaks' material embarrassed the DNC and the Clinton campaign, but the rupture of secrets was not considered a very important factor in Clinton's loss to Donald Trump. Clinton herself blamed that surprising outcome on FBI Director James Comey's last-minute decision to briefly reopen the investigation into her improper use of a private server for her emails as Secretary of State.

After Comey's move, Clinton's poll numbers cratered and she seemed incapable of reversing the trend. More generally, Clinton faced criticism for running an inept campaign that included her insulting many Trump supporters by calling them "deplorables" and failing to articulate a clear, hopeful vision for the future.

However, after the shock of Trump's stunning victory began to wear off, the outgoing Obama administration and angry Democrats began singling out Putin as a chief culprit in Clinton's defeat.

Despite the appearance that they were scapegoating America's old adversary – the Russkies – liberals and Democrats have used the allegations to energize their base and put the young Trump administration on the defensive, even though hard evidence to support the accusations is still lacking.

The liberals and Democrats also don't seem to care that they are using these dubious allegations to ratchet up tensions between the world's two nuclear superpowers, thus putting the future of the world at risk.

Investigative reporter Robert Parry broke many of the Iran-Contra stories for The Associated Press and Newsweek in the 1980s. You can buy his latest book, *America's Stolen Narrative,* either in print here or as an e-book (from Amazon

and barnesandnoble.com).