Russians Spooked by Nukes-Against-Cyber-Attack Policy

New U.S. policy on nuclear retaliatory strikes for cyber-attacks is raising concerns, with Russia claiming that it's already been blamed for a false-flag cyber-attack – namely the election hacking allegations of 2016, explain Ray McGovern and William Binney.

By Ray McGovern and William Binney

Moscow is showing understandable concern over the lowering of the threshold for employing nuclear weapons to include retaliation for cyber-attacks, a change announced on Feb. 2 in the U.S. Nuclear Posture Review (NPR).

Explaining the shift in U.S. doctrine on first-use, the NPR cites the efforts of potential adversaries "to design and use cyber weapons" and explains the change as a "hedge" against non-nuclear threats. In response, Russia described the move as an "attempt to shift onto others one's own responsibility" for the deteriorating security situation.

Moscow's concern goes beyond rhetoric. Cyber-attacks are notoriously difficult to trace to the actual perpetrator and can be pinned easily on others in what we call "false-flag" operations. These can be highly destabilizing – not only in the strategic context, but in the political arena as well.

Russian President Vladimir Putin has good reason to believe he has been the target of a false-flag attack of the political genre. We judged this to be the case a year and a half ago, and said so. Our judgment was fortified last summer – thanks to forensic evidence challenging accusations that the Russians hacked into the Democratic National Committee and provided emails to WikiLeaks. (Curiously, the FBI declined to do forensics, even though the "Russian hack" was being described as an "act of war.")

Our conclusions were based on work conducted over several months by highly experienced technical specialists, including another former NSA technical director (besides co-author Binney) and experts from outside the circle of intelligence analysts.

On August 9, 2017, investigative reporter Patrick Lawrence summed up our findings in The Nation. "They have all argued that the hack theory is wrong and that a locally executed leak is the far more likely explanation," he explained.

As we wrote in an open letter to Barack Obama dated January 17, three days

before he left office, the NSA's programs are fully capable of capturing all electronic transfers of data. "We strongly suggest that you ask NSA for any evidence it may have indicating that the results of Russian hacking were given to WikiLeaks," our letter said. "If NSA cannot produce such evidence – and quickly – this would probably mean it does not have any."

A 'Dot' Pointing to a False Flag?

In his article, Lawrence included mention of one key, previously unknown "dot" revealed by WikiLeaks on March 31, 2017. When connected with other dots, it puts a huge dent in the dominant narrative about Russian hacking. Small wonder that the mainstream media immediately applied white-out to the offending dot.

Lawrence, however, let the dot out of the bag, so to speak: "The list of the CIA's cyber-tools WikiLeaks began to release in March and labeled Vault 7 includes one called Marble Framework that is capable of obfuscating the origin of documents in false-flag operations and leaving markings that point to whatever the CIA wants to point to."

If congressional oversight committees summon the courage to look into "Obfus-Gate" and Marble, they are likely to find this line of inquiry as lucrative as the Steele "dossier." In fact, they are likely to find the same dramatis personae playing leading roles in both productions.

Two Surprising Visits

Last October CIA Director Mike Pompeo invited one of us (Binney) into his office to discuss Russian hacking. Binney told Pompeo his analysts had lied and that he could prove it.

In retrospect, the Pompeo-Binney meeting appears to have been a shot across the bow of those cyber warriors in the CIA, FBI, and NSA with the means and incentive to adduce "just discovered" evidence of Russian hacking. That Pompeo could promptly invite Binney back to evaluate any such "evidence" would be seen as a strong deterrent to that kind of operation.

Pompeo's closeness to President Donald Trump is probably why the heads of Russia's three top intelligence agencies paid Pompeo an unprecedented visit in late January. We think it likely that the proximate cause was the strategic danger Moscow sees in the nuclear-hedge-against-cyber-attack provision of the Nuclear Posture Statement (a draft of which had been leaked a few weeks before).

If so, the discussion presumably focused on enhancing hot-line and other fail-safe arrangements to reduce the possibility of false-flag attacks in the strategic arena – by anyone – given the extremely high stakes.

Putin may have told his intelligence chiefs to pick up on President Donald Trump’s suggestion, after the two met last July, to establish a U.S.-Russian cyber security unit. That proposal was widely ridiculed at the time. It may make good sense now.

Ray McGovern, a CIA analyst for 27 years, was chief of the Soviet Foreign Policy Branch and briefed the President’s Daily Brief one-on-one from 1981-1985. William Binney worked for NSA for 36 years, retiring in 2001 as the technical director of world military and geopolitical analysis and reporting; he created many of the collection systems still used by NSA.