Biden's Cyberattack Hypocrisy. "The Russians are Coming"

By Kurt Nimmo
Global Research, March 26, 2022
Region: Europe, Russia and FSU, USA
Theme: Intelligence

***

On Monday, President Joe Biden said "evolving intelligence" indicates Russia is preparing a massive cyberattack against the United States in response to its support for Ukraine. "The magnitude of Russia's cyber capacity is fairly consequential and it's coming," Biden said.

Days prior to Biden's remarks, an FBI advisory issued to US businesses warned "Kremlin-linked hackers could target US organizations as the Russian military continues to suffer heavy losses in Ukraine and as Western sanctions on the Kremlin begin to bite," reports CNN.

Anne Neuberger, Biden's national security adviser, said during a White House press briefing on Monday Russia is preparing "preparatory activity" for a cyber attack on the United States and its allies. She declared the coming attacks are "not about espionage, it's probably very likely about disruptive or destructive [cyber] activity" in response to US assistance to Ukraine. The following day, US Cybersecurity and Infrastructure Security Agency Director Jen Easterly made similar remarks to business executives, according to CNN.

(It should be noted Neuberger is a Zionist and thus an ardent defender of Israel; the Yehuda and Anne Neuberger Foundation has "donated hundreds of thousands of dollars to American Israel Public Affairs Committee, the pro-Israel lobby known as AIPAC, for its efforts to influence the US government and public opinion," David Corn reported for Mother Jones in 2021.)

NATO Secretary General Jens Stoltenberg said in February a Russian cyberattack "on one will be regarded as an attack on all," a statement that invokes NATO's Article 5 of the Washington Treaty. "Article 5 provides that if a NATO Ally is the victim of an armed attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked," explains the NATO web page.

The United States, and especially Joe Biden and his son, Hunter Biden, have a vested

interest in making certain Volodymyr Zelenskyy and the color revolution installed government of Ukraine remain in power.

The fact is the US, under the State Department and Obama's Assistant Secretary of State for European Affairs, Victoria Nuland, and the US Ambassador to Kyiv Geoffrey Pyatt, were responsible for orchestrating the overthrow of the democratically elected government of President Viktor Yanukovych.

This is a taboo subject for the corporate media as it reports a one-sided blow-by-blow account of the war in Ukraine. Never mentioned is the fact the US orchestrated color revolution in Ukraine (and those in Georgia and Kyrgyzstan) violate the United Nations Charter and international law.

Prior to leaving office, President Obama looked into "an unprecedented cyber covert action against Russia in retaliation for alleged Russian interference in the American presidential election, U.S. intelligence officials told NBC News." As we now know—and some of us claimed at the time—the supposed effort by Russia to get Donald Trump elected was pure fantasy and rank political expediency. It took almost two years for ex-FBI Director Robert Mueller to discover the obvious—there had been no collusion between Trump's campaign and Russia. Despite this, many Americans, in particular Democrats, believe the conspiracy theory is true.

The effort to destabilize Russia continued under the outlier president Trump. He gave the CIA carte blanc to launch cyber attacks on Russia. "The secret authorization, known as a presidential finding, gives the spy agency more freedom in both the kinds of operations it conducts and who it targets, undoing many restrictions that had been in place under prior administrations. The finding allows the CIA to more easily authorize its own covert cyber operations, rather than requiring the agency to get approval from the White House," reported Yahoo News in 2020.

The "very aggressive" finding "gave the agency very specific authorities to really take the fight offensively to a handful of adversarial countries," said a former U.S. government official. These countries include Russia, China, Iran and North Korea — which are mentioned directly in the document — but the finding potentially applies to others as well, according to another former official. "The White House wanted a vehicle to strike back," said the second former official. "And this was the way to do it." (emphasis added.)

Those of us who study history and geopolitics know the CIA has had a free hand to conduct subversion and surveillance activities around the world and at home despite its charter. "When the CIA was created in 1947, members of Congress who feared the establishment here of the type of domestic surveillance apparatus that the Allies had just defeated in Germany insisted that the new CIA have no role in American law enforcement and no legal ability to spy within the U.S. The legislation creating the CIA contains those limitations," writes Andrew Napolitano.

> "Populations from at least 25 countries were denied the right to choose their own leaders," writes Thomas Swan. "This is perhaps the main reason why America is hated so much around the world. The excuse given by CIA supporters is that Soviet influence over certain governments had to be curtailed. However, in many cases, no proof of Russian activity was ever found. The CIA had taken to dismantling any leftist or anti-US

> government, regardless of the regime's domestic or foreign support."

The CIA, following Trump's "presidential finding," engaged in a new round of computer and network subversion against Russia and Iran. The 2018 finding gave a green light to the CIA to wipe or dump hacked banking data and target foreign intelligence services, media organizations, charities, religious institutions, or other non-state entities for disruptive or destructive cyber actions, according to a report posted at Axios.

In fact, Trump's finding was little more than a formality. In addition to overthrowing elected governments, the CIA has engaged in assassination, the distribution of heroin and cocaine, and making certain local officials, most notably state governors, are onboard with the establishment's program (see "Former Governor Jesse Ventura Explains That CIA Embedded In Many State Governments").

> "Recently we have noted a significant increase in attempts to inflict harm on Russia's informational systems from external forces," Nikolai Patrushev, secretary of Russia's Security Council, told the Rossiiskaya Gazeta daily in January of 2017, prior to the US election. Patrushev said the Obama administration had "deliberately ignor(ed) the fact that the main Internet servers" complicit in the attacks "are based on the territory of the United States and are used by Washington for intelligence and other purposes aimed at retaining its global domination."

In short, the intelligence apparatus of the US was engaged in subverting Russia's computer networks (and those in China, Iran, and North Korea) years before the current crisis in Ukraine and the contested US election. This was accomplished under the bogus assertion that Putin and Russia colluded with the Trump team to get him elected, thus painting the real estate magnate as a Russian tool.

"The U.S. CIA's hacking unit has been conducting attacks over the last 11 years on Chinese aviation firms, technology companies, oil sector companies and other critical industries," Emily Fang, a correspondent in Beijing, told NPR in 2021.

China, Russia, North Korea, Israel, and other nations have probed the networks of adversaries for years, and may have indeed engaged in cyberattacks. However, as Wikileaks discovered in 2017, the CIA is at the forefront of this activity. Its sophisticated arsenal of cyberattack tools include "malware, viruses, trojans, weaponized 'zero day' exploits, malware remote control systems," according to WikiLeaks "Vault 7" archive of documents purloined from the CIA.

The "Year Zero" documents introduce "the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of 'zero day' weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones."

The events of 9/11 gave the agency the emphasis it needed to expand its cyberattack efforts.

Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force — its own substantial fleet of

hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.

All of the above represents factual information, not a conspiracy theory. I believe—and this is my opinion based on years of dedicated research—that the majority of cyberattacks launched against US corporations and the government originated with CIA hackers who leave behind traces implicating the above roster of official enemies.

In the days to come, as the war in Ukraine continues, we may face cyberattacks on critical infrastructure here in the US. The warfare state is dedicated to confronting Russia and China, even if it results in a nuclear conflagration. There is no better way to get Americans onboard with criminal behavior than to let them sit in the dark for a week or more without access to streaming television and their precious smart phones that are in effect surveillance devices.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @globalresearch_crg and Twitter at @crglobalization. Feel free to repost and share widely Global Research articles.

Kurt Nimmo is a regular contributor to Global Research.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Kurt Nimmo