Neocons CONCOCT Threat of "Iranian Hackers" to Justify Preemptive "Counterattack" Against Iran

by Whitney Webb via gus - Mint Press News *Thursday, Aug 9 2018, 10:37pm*
international / prose / post

> *It now is confirmed, the neocons have learned nothing as the public did not follow through on their heinous crimes in duping the USA and its vassals that Iraq had "WMD", a fabricated LIE, or that invading Iraq would be a "cakewalk," and that the people of Iraq would welcome US invaders with "bouquets of flowers," -- give the world a break you lying, mass murdering NEOCONS. The world would soon regret not hauling responsible known neocons before the courts for their duplicitous lying regarding unnecessary illegal invasions of other States which have NEVER posed a threat to the USA or Europe, and which illegal invasions resulted in millions of innocent deaths and tens of millions more displaced persons -- refugees.*

Arch-neocon, John Bolton -- 'political ignoramus Trump, is easy to play!'

Try it again neocons, BUT this time using old TIRED tricks would see you in the courts, even Murdoch knows that such overt LIES are a once-only venture. Though at least you have the Washington Post and New York Times to do your nefarious bidding today. Give it a shot, please!

MPN Article follows:

> Several reports in both American and Israeli media have recently been circulating the claim that Iran is increasingly likely to respond to draconian U.S.-imposed sanctions by conducting "cyberattacks" against the United States. According to this narrative, "Iranian hackers have laid the groundwork to carry out extensive cyberattacks on U.S. and European infrastructure and on private companies," prompting the U.S. to consider launching a preemptive "counterattack" in response.
>
> Quoting anonymous U.S. government officials, think tanks and "experts," these articles assert that the sanctions the U.S. re-imposed on Iran this Tuesday are "likely to push that country to intensify state-sponsored cyber-threat activities," activities that one expert called "the most consequential, costly and aggressive in the history of the internet, more so than Russia."
>
> However, upon closer examination, it is clear that these warnings of an imminent Iranian

cyberattack are dubious at best — aimed at ending the U.S.' isolation on the issue through dishonest intelligence, while also justifying a U.S. "preemptive counterattack" on Iran's infrastructure in a bid to further destabilize the nation, in service to the Trump administration's overall goal of regime change in Iran.

Chatter by whom?

Most of these articles, in introducing the "threat" posed by Iranian state-sponsored hackers, state that they originated with "cybersecurity and intelligence experts." However, just sentences later, when these experts are quoted they specifically state that no evidence of such a threat even exists.

For instance, an Associated Press story, which begins with the statement that "the United States is bracing for cyberattacks Iran could launch in retaliation for the re-imposition of sanctions," quotes Priscilla Moriuchi — director of strategic threat development at Recorded Future, a cyber-threat intelligence company — as saying the following just two sentences later:

"*While we have no specific threats, we have seen an increase in chatter related to Iranian threat activity over the past several weeks.*"

In saying so, Moriuchi essentially admits that there is no threat from Iranian hackers, merely stating that there has been a jump in "chatter" related to Iranian threat activity. Notably, the "chatter" is not attributed, meaning that this increase could be a result of U.S. or Israeli intelligence hyping the possibility of a threat, not necessarily Iranians or their allies threatening a cyberattack.

Considering the source

Furthermore, Moriuchi is hardly unbiased, as her company, Recorded Future, counts among its clients several U.S. weapons manufacturers like Raytheon, and also regularly collaborates with the U.S. Department of Homeland Security as well as technology companies that double as U.S. military contractors, such as Google and Palantir. Notably, Recorded Future was initially funded by both Google and In-Q-Tel, the venture-capitalist arm of the Central Intelligence Agency (CIA).

In addition, this report and others rely on the analysis of equally flawed "experts" to make their case. For instance, NBC cites "Iran expert" Behnam Ben Taleblu, who states that "Iran has a penchant for using such tools against the West." However, Taleblu is a fellow at the Foundation for Defense of Democracies (FDD), the hawkish neo-conservative think tank that has long championed preemptive bombings against Iran.

The FDD is so stacked with notorious neo-conservatives that it has long been called the successor to the now-defunct think tank Project for a New American Century (PNAC), which was instrumental in promoting the invasion of Iraq under false pretenses. The FDD is also closely associated with National Security Adviser John Bolton, who promised just last year that the Iranian government would be toppled before 2019. However, NBC left out this important context, merely calling the FDD "a conservative think tank in Washington."

Another "expert" quoted in these articles was Norm Roule, who was introduced as "the former Iran manager for the office of the Director of National Intelligence." Roule, who

recently told the press that he believes that Iran “will muster its cyberforces in response” to U.S. sanctions, is a 34-year veteran of the CIA and, more importantly, a https://www.thecipherbrief.com/experts/norman-t-roule senior adviser to the group United Against Nuclear Iran (UANI).

UANI is a think tank stuffed to the brim with Iran hawks, counting among its current members former Senator Joseph Lieberman; Richard Dearlove, former head of the UK’s MI6; Tamir Pardo, former general director of Israel’s Mossad; and Jeb Bush. UANI was originally co-founded by Richard Holbrooke, John Bolton and Meir Dagan — another former general director of the Mossad. Thus, given their associations to organizations that have long promoted the destruction of the Iranian state, Roule’s analysis, much like Taleblu’s, can hardly be considered impartial or objective.

Self-isolated U.S. seeks a way out of the trap

The U.S.’ warning of an imminent Iranian cyber-threat in response to the U.S.’ decision to withdraw from the Joint Comprehensive Plan of Action (JCPOA), better known as the Iran nuclear deal, and its subsequent decision to reimpose harsh sanctions against the Islamic Republic, comes at a crucial time, as many key countries, including many important U.S. allies, have declined to follow the U.S.’ lead on isolating Iran and have even rejected it outright.

Indeed, as opposed to isolating Iran, the U.S. has become isolated itself, as E.U. countries have banned companies from complying with U.S. sanctions efforts and other key nations like China have refused to halt Iranian oil imports despite U.S. threats. However, were U.S. warnings of an “Iranian cyber-threat” to convince these countries, particularly Europe, that Iran was indeed on the offensive despite its desperate efforts to keep JCPOA alive, the U.S.’ isolation in terms of its Iran policy could well end.

The Iranian government seems to have caught on to the U.S.’ game but seemed to think that rather than simply being intended to intensify Washington’s isolation campaign, the fear mongering over “Iranian hackers” was aimed at justifying imminent U.S. aggression against Iran.

In a statement given to NBC by Alireza Miryousefi, spokeswoman for Iran’s UN delegation, she stated that “Iran has no intention of engaging in any kind of cyber war with the U.S.,” adding, “from our perspective, it’s more likely the U.S. wants the supposed suspicion of an attack as rationalization for a cyberattack against Iran.” Miryousefi went on to call the U.S. “the most belligerent cyber-attacker of any nation in the world, repeatedly attacking military and civilian targets across the world, including in Iran.”

Indeed, the U.S. famously targeted Iran’s civilian nuclear program with the Stuxnet virus it had jointly developed with Israel. It infected over 200,000 machines and destroyed around 20 percent of Iran’s nuclear centrifuges.

Perhaps unsurprisingly, mass media reports themselves hint that this is the case, stating that while “the U.S. has not yet decided whether it will retaliate in the event of an attack,” it is already preparing new sanctions to impose on the country whether or not an attack occurs and is also building “a case for its more confrontational stance” in a bid to convince its wary allies to join its aggressive Iran policy.

> The reports also openly state that a “preemptive attack” against Iran is currently being debated by the Trump administration, but notes that officials are “divided” over the measure. However, given the increasing likelihood that Secretary of Defense James Mattis, who had supported JCPOA, is on the way out of the administration, the growing chorus of Iran war-hawks in the White House could soon make such “divisions” a thing of the past.

https://www.mintpressnews.com/neocons-hype-threat-of-iranian-hackers-to-justify-preemptive-counterattack/247369/
