From Cyberwar to Nuclear War?

by Barbara Boyd

June 23—Lyndon LaRouche often described witnessing the sea change that came over the American population when it was announced that the Japanese had attacked the U.S. fleet in Pearl Harbor. In New York City, during the afternoon of December 7, 1941, LaRouche witnessed a population which, just moments before, had been preoccupied by life's everyday activities, suddenly confronting a dramatically changed future with stunned absolute silence, solemnity, and determination.

On Friday, President Donald Trump called off U.S. military strikes on the nation of Iran after, it was claimed, the Iranians shot down an unarmed U.S. drone. The President, in a tweet, recounted his decision. How many people would be killed by the planned action? the President asked the Generals. They came back with the answer, "150, sir." He thought for a moment, the President said in his tweet, and said, "No." He added, "I didn't think it was proportionate." So, Washington's armchair warriors had proposed that the United States kill 150 people over the shooting down of an inanimate object, a drone, which, they argued, cost a ton of money. In calling off the military strikes, the President told the public that he made the "common sense" decision any human would make in such a situation.

The intelligence community and news media—one cohesive, incestuous entity in the United States—and their British imperial masters, are furious about this President's courageous decision and most important, the President's direct discussion with the American public about it, mostly via twitter. It is a direct challenge to the mental and human capacities of the Anglo-American elite.

Did the President really abandon the so-called principals and advisors that have endlessly trapped Presidents in wars, and did he listen, instead, to his own judgment?—President Trump's opponents rage. Was he influenced by Fox News Host Tucker Carlson, telling him on Fox TV over the three nights prior to Friday's decision, lurid details about the lust for war that dominates official Washington, something the President himself has publicly condemned? Carlson argued repeatedly, that the larger war with Iran—ached for by official Washington and London, a war that would kill millions while giving Washington's war hawks a "rush"—would also doom the President's electoral prospects and his legacy.

Oh, how offensive and dangerous to official Washington—to the Mandarins steeped in British geopolitical doctrines and in the practice of "managing" populations, imperial wars, and American presidents! Was Iran's shootdown really a mistake by a rogue Iranian military element, pronounced as a "theory," by President Donald Trump and as "fact" by General Jack Keane who backed the President up in TV appearances? Who in the hell, the Mandarins ask, leaked that?

Surveillance State Under Examination

This article is the first in a series of examinations of the surveillance state—the realm of cyber and information warfare in which an actual war is now being fought. It is a battle for the mind of the American public, primarily, which has been dramatically escalated by the British in the wake of China's Belt and Road Initiative and the partial failure of the Anglo-American 2014 coup in Ukraine. It encompasses the illegal operations against the Trump Campaign and Presidency and the false-flag tarring of the Russians for malign election interference in 2016, when the real culprit was the desperate effort of the British and aligned intelligence services to swing the election to Hillary Clinton.

This war is now fully underway in the censorship regimes undertaken by Google, Facebook, et al., in direct alliance with the British government to de-platform and censor voices dissenting from the war aims of the British imperial forces. The British House of Lords itself proclaimed one aspect of this drive in its 2018 report, "British Foreign Policy In a Shifting World Order," by openly declaring control of social media essential to defeating Donald Trump and managing the dissenting population that elected Trump in the United States, which widespread dissent also exists worldwide as a source of resistance to deadly imperial plans. It also encompasses a new and dangerous cyberwarfare doctrine embraced and escalated by the Congress and the

"Five Eyes" intelligence community, using the fake Russiagate information-warfare operation as a pretext.

Those cyberwarfare doctrines are the subject of this article and were put on the public's plate by the June 15 *New York Times* article that claims the U.S. Cyber Command has placed crippling malware into the Russian power grid controls, without explicit Presidential approval.

In fact, the *Times* article states, the President was not briefed explicitly because he might reverse these actions or tell the Russians about them. Can this moment wake us up, like the Pearl Harbor moment Lyndon LaRouche described? Well, it needs to—and this can only happen if the American public mobilizes against its real enemy, the imperial entity that controls the world's money and finances and controls populations through psychological warfare and by shaping and controlling public opinion. It can if the American population mobilizes to cause the exoneration of Lyndon LaRouche and thereby liberates the treasure trove of policies and ideas, which this President can wield to finally defeat our nation's historical enemy.

For those who don't know by now, the imperial opponents of LaRouche sought to eliminate his ideas through demonization and a monstrously illegal criminal prosecution, akin in its mechanisms to the atrocity they have now attempted to stage against Donald Trump and his supporters. Now, we finally have a President who will fight these ghouls, as he has repeatedly demonstrated. If you add LaRouche's ideas and policies to the President's intelligence and guts, victory can, finally, be ours.

Cyber Command Offensive Against Russia

The gravamen of the June 15 *New York Times* article is that the U.S. Cyber Command—under the command of General Paul Nakasone, who also serves as the Director of the National Security Agency (NSA) and Chief of the Central Security Service—has undertaken offensive cyberwarfare activities on a scale not seen before that now includes the planting of disabling malware in the Russian power grid controls and other Russian systems. According to Nakasone's bellicose and stupid Congressional testimony, the Russians "do not fear us" and that needs to change.

The rationale the *Times* and other outlets covering this classified leak offer for the offensive cyber actions is confused. It variously claims that this is punishment of the Russians for the cyberattacks falsely attributed to Russia in the 2016 U.S. Presidential election, and was done as a warning not to repeat such activities in the 2018 midterm elections, or that it is offensive preparation of the battlefield for a future war. The *Times* recounts a slew of alleged Russian cyber intrusions into the U.S. power system, infrastructure, and nuclear plants in addition to the alleged election meddling. The *Times* claims that President Trump was not briefed "in detail" about offensive cyber actions against the Russians—which most would consider a retaliatory act of war. The *Times* goes on to cite the National Defense Authorization Act of 2019 and National Security Presidential Memorandum 13, a classified document, which followed the National Defense Authorization Act (NDAA), as the authorization permitting the cyber commander, General Nakasone, or the Secretary of Defense, to order offensive cyber actions without Presidential approval. In response, President Trump tweeted that the *Times* story was an act of treason and, also, that it was not true.

There are several key dates in the run-up to the events claimed in the *New York Times* story.

Obama's Offensive Cyber-Ops

First, it should be noted that offensive cyber operations were conducted by the Obama Administration in an escalating fashion beginning in 2012. According to reliable sources in the intelligence community, cyber-surveillance inside a potential adversary's essential infrastructure systems has been a common practice of major states, including the United States, Russia, China and Israel, for some years. Nonetheless, offensive cyberwarfare operations were rare.

That changed with the British Russiagate operation conducted in 2016 against the United States. Allegedly as punishment for the Russian hack—which never happened—of the DNC and John Podesta, Barack Obama placed malicious code into the Russian power grid controls to be activated by President Trump or a future U.S. President. That "sanction" was included in the package of Russiagate sanctions that saw the expulsion of many Russian diplomats from the United States by Obama. Despite the hysteria in the press and the Congress generated by Russiagate, President Trump refused to escalate cyberwar against the Russians. In the legislative run-up to the 2019 NDAA, the Conference Committee putting the legislation into final form criticized the Administration's "stalling" tactics. The Senate and House conferees said that the President refused to take Russian's malign meddling the in the 2016 election seriously and had not complied with Congressional demands for detailed plans for both cyber security and retaliatory actions. According to the Congress, President Trump provided nothing but a vague summary of possible future plans and 60

pages of recommendations for further study.

On May 24, 2018, British Attorney General Jeremy Wright QC (Queens Counsel), Member of Parliament (MP), publicly announced the United Kingdom's position on applying international law to cyberspace. To make a long story short, the official British position is that British offensive cyberwarfare need not follow international law. In response to a cyberattack and in consideration of "countermeasures," the British say they are not required, as they would be under international law, to give the attacking state notice before taking countermeasures against it.

They also state that a cyber response need not be "symmetrical" to the underlying unlawful act. This is consistent with the incorporation of British policies in the 2018 U.S. Nuclear Posture Review, arguing that nuclear weapons could be deployed in the wake of a devastating cyberattack on fundamental infrastructure. To make the British direction of U.S. policy absolutely clear, consider the fact that British intelligence and cyber operatives perennially occupied an entire floor of the NSA, right below the Director's offices. It should also be noted that under the British "laws" of cyberwar, the placing of malicious malware in a potential adversary's vital infrastructure systems is not an act of war unless it is activated.

National Defense Authorization Act

The NDAA for 2019 began its journey through the Congress with a House vote in April 2018 amidst the full hysteria surrounding Russiagate. It is called, appropriately, the John S. McCain National Defense Authorization Act of 2019, after the bellicose Arizona Senator who hated Donald Trump and never saw an opportunity for war he wasn't prepared to inflame. Thereafter, the U.S. Senate steered the bill toward the use of offensive cyberwar, while specifically targeting Chinese tech giants Huawei and ZTE for economic warfare. Robert Chesney, a law professor at the University of Texas, who has examined the cyberwarfare provisions Congress put into the NDAA, says that while Congress can't make the President satisfy their lust for offensive cyberwar, Section 1642 of the NDAA amounts to an authorization of "proportional" cyberwar by the Defense Department in response to Russian, Chinese, North Korean and Iranian cyber activities. Let that sink in, Congress is granting a war power to the Defense Department, to circumvent non-action by a President.

Critical to Congress's cutting the President out of the cyber war approval chain was the NDAA's recasting of most aspects of cyberwar as "traditional military activity," rather than covert action, which requires a Presidential finding. Traditional military activities do not require any form of notification of the President and include, according to Congress, "forward preparation of the adversary's battle space" and placing malware, which has not been activated.

Additionally, the Secretary of Defense was added to the "command authority" explicitly reserved for the President in ordering active and destructive modes of cyberwarfare after hostilities commence. According to an August 15, 2018 article in the *Wall Street Journal*, John Bolton, a hod carrier for British warfare policies throughout his long career, campaigned from the beginning of his term as National Security Advisor, in April of 2018, for a streamlined command authority for cyberwarfare, eliminating the "cumbersome" approval process under Obama.

Now flash forward to July 16, 2018 as President Trump and Russian President Vladimir Putin met in Helsinki. On the Friday before, July 13, Special Counsel Robert Mueller had indicted 12 Russians for the DNC hack that never happened, in a clear attempt to poison the prospects for the summit. Nonetheless, the two Presidents emerged to declare to the world that they wished to establish working groups to discuss de-escalating cyberwar, an urgent necessity for humanity based on all that I have just told you about.

President Trump also said that he accepted President Putin's strong denial that the Russians had hacked the DNC, and both discussed a plan whereby U.S. prosecutors could interview the 12 Russians indicted by Mueller, and the Russians could interview Anglo-American assets Michael McFaul and Bill Browder, who have led the charge for regime change in Russia. The international news media, the Anglo-American intelligence apparat, and virtually the entirety of the U.S. Congress went absolutely ballistic after the press conference, declaring that Putin had eaten Trump's brain and that the President was clearly demonstrating that he was nothing but a stupefied pawn of the Russian president. The President signed the NDAA into law on August 13, 2018, waiting to fight another day.

That day has now come. Attorney General William Barr is promising to expose all of the elements of the coup that was run against this President, including its British imperial components. The President has, once again, told the war party "No!"—because humanity is something alien to them. And, now, it is very much a battle that can be won, provided the American people approach it with openness, intelligence, and creativity, and with the steely and solemn determination to learn and to win, which Lyndon LaRouche witnessed on December 7, 1941.