Hypocrisy Over Alleged Russian ‘Hacking’

As Official Washington rages over alleged Russian hacking of Democratic emails, a forgotten back story is how the U.S. government pioneered the tactics of cyber-war and attacked unsuspecting countries, recalls Michael Brenner.

By Michael Brenner

The psychodrama over the alleged but unsubstantiated Russian hacking of Democratic emails to influence the U.S. presidential election has yet to reach its climax. Already, though, it has earned nomination as the most surreal and passionate work of fiction of the Twenty-first Century.

In all the excitement, it is easy to lose perspective. Perhaps the biggest piece of the untold story is the United States government’s pioneering role in electronic surveillance and hacking. We seem to have forgotten that the National Security Agency and the Central Intelligence Agency eavesdropped on heads of state in Germany, Brazil, Argentina, Iraq, Venezuela – and, at last count, several score other capitals. Also, the United Nations Secretary General, the President of the European Union Commission, the European Central Bank and God knows whom else.

This was not coincidental. It was part of a calculated strategy approved by two successive Presidents to monitor all electronic communications around the globe. Author James Bamford and other knowledgeable experts have provided us with a detailed history of the program.

Yet, the U.S. – as presented to us by the mainstream media and most commentators reflecting Official Washington –is portrayed as the innocent among the main protagonists. The plot line represents America as the victim of unprovoked cyber aggression by the Russians and, in other circumstances, the Chinese – these attacks coming out of the blue, an aggressive blow in an assumed contest for global dominance between the powers.

Is any of this true? Frankly, we haven’t even seen the proof. But let’s assume that there is an element of truth to it (leaving apart the nonsense about a Kremlin plot to manipulate and then destroy American democracy).

On the Offensive

Let us recall that it was the United States that launched the first cyber attacks – some years ago by the NSA. This history is detailed in the Snowden documents whose authenticity never has been questioned. We succeeded in trespassing on the computer networks of several Chinese government agencies and

individuals. We boasted about our success in intra-governmental communications. Those occurred at a time when related documents now in the public realm revealed the NSA's ambition to tap into every electronic communications network in the world and laid out a program for achieving that goal.

Simultaneously, the United States was launching ***offensive assaults*** on Iran. The targets there included not just their nuclear research facilities but also critical centers for the oil and gas industry. These are acts of war. Yet there was never a mandate from any international body for doing so, nor a *casus belli*. We did it in collaboration with the Israelis because we made the unilateral judgment that aggression was in our national interest. Now we are outraged that others are doing what we have done. This is rank hypocrisy. It also is not very bright. For the initial actions made the casual assumptions that the U.S. would always have an advantage; therefore, the setting of norms and rules was unnecessary and undesirable. The same logic operated in regard to drones and targeted assassinations.

Conditions now have changed and the now U.S. is vulnerable to attack. The option of negotiating international rules of the road and perhaps formal regulations is slipping away. We will have to live with the chaotic mess that we have created.

Whatever thinking the NSA did on the subject (and perhaps other agencies) bears an uncanny resemblance to Air Force General Curtis LeMay's attitude toward nuclear strategy: An emphasis on offense because it played to our advantage; defense only in the form of "massive retaliation" which – for Lemay – was the strategic cover for massive first strike; and a conviction that this was an unavoidable zero-sum game played for the highest stakes. In other words, cowboy strategy. And it is cowboy strategic thinking that has ruled in the NSA.

Cyber Army

The most revealing article on this appeared in *WIRED* in July 2014 by James Bamford. Army General Keith Alexander, who was NSA director from 2005 to 2014, revealed the full scope of his ambition. Here are some of the article's more noteworthy quotes: "For years, U.S. General Keith Alexander has been amassing a secret cyber army. Now it's ready to attack. … Alexander's forces are formidable – thousands of NSA spies, plus 14,000 cyber troops. … Endgame hunts for hidden security weaknesses that are ripe for exploitation."

Plans included a "launch on warning" doctrine calling for a massive cyber-retaliation against anyone who launched a strategic attack on sensitive U.S. computers. Its code name was "MonsterMind." But preparations for the Great Cyber War evidently left no time to keep track of smaller attacks (such as the alleged hacking of Democratic emails) or else its radar was badly defective.

[Also see *THE INTERCEPT* of Oct. 10, 2014, "Core Secrets: NSA Saboteurs in China and Germany" by Peter Maass and Laura Poitras.]

Michael Brenner is a professor of international affairs at the University of Pittsburgh. *mbren@pitt.edu*