US media escalate anti-China propaganda over alleged hacking

Thomas Gaist
6 June 2015

After receiving a quiet go-ahead from the Obama administration this week, the *New York Times*, the *Washington Post* and the US television networks trumpeted unsubstantiated accusations that Chinese hackers have stolen personal data on millions of government employees from US government servers.

The alleged cyberattacks, which the corporate media strongly suggests have originated with the Chinese government, supposedly involved lifting files on some 4 million federal workers from servers of the Office of Personnel Management.

While the Obama administration has stopped short of directly accusing the Chinese government of involvement in the hacking, belligerent voices in the media and political establishment are already speaking as if Beijing's involvement is certain.

None of the media reports is based on actual journalism. Instead, the reporters involved, whether at the major daily newspapers or the television networks, are taking their cues from the White House, the Pentagon and the Central Intelligence Agency (CIA).

The report by the *New York Times*, for example, "Chinese Hacking of US Data May Extend to Insurance Companies," has all the appearances of a semi-official US government press release. It lays out, not demonstrable facts, but rather an argument that serves the political aims of the US ruling class.

In the upside down, war-mongering narrative advanced by the *Times*, a growing wave of Chinese cyberattacks has been launched against the US, in spite of supposed efforts by the Obama administration to de-escalate cyber-tensions between the two governments.

"The intrusions also suggest that President Obama's efforts over the past three years to engage China's leadership in a dialogue that would limit cyberattacks has failed. The pace of the attacks is unabated, and the scope has grown," the *Times* warned.

Painting the alleged hacks in grandiose and ominous terms, the *Times* proclaimed that the world is facing a "new era in cyberespionage," in which the US population at large will face cyberattacks similar to those allegedly launched against US business and state institutions in recent years.

"Spies are no longer stealing just American corporate and military trade secrets, but also personal information for some later purpose," the newspaper warned. "The attackers seem to be amassing huge databases of personal information about Americans."

Readers should perhaps stop now to rub their eyes in disbelief. Only a few days ago, the main news story in the United States was the effort of the US National Security Agency to "amass huge databases of personal information about Americans."

Moreover, this was accomplished, not by a murky hacking operation, but by a massively funded government program, authorized at the highest levels, that seized all telecommunications and Internet data generated by all telecoms, ISPs and corporations like Google and Yahoo!

The legislation signed into law by Obama Tuesday, and hailed by the *Times* as a breakthrough for civil liberties, only changed one aspect of this massive surveillance operation—described by the NSA internally as an effort to "capture it all"—by shifting responsibility for collecting telephone metadata from the NSA to the telecoms. All other NSA programs to spy on the American people and the population of the world continue entirely as before.

The media attack on China thus serves two purposes: to distract attention from the real and growing threat to democratic rights and privacy in the United States, which comes from Washington, not Beijing, and to

further the campaign of anti-Chinese provocation and saber-rattling which the Obama administration calls its "pivot to Asia."

Whatever the reality of the latest hacking allegations, the attribution to China is extremely dodgy and unsubstantiated. While the *Times* assured readers that there is "little doubt among federal officials" that the attacks were launched from China, it acknowledged that the White House has declined to publicly finger the Chinese state as the source "because of a broader diplomatic strategy."

In part, the unwillingness of the White House to publicly stand behind the accusations against the Chinese government, even as the American corporate media screams at them at the top of its lungs, is a demonstration of the extremely inflammatory nature of the charges, which verge on declaring that China is at war with the United States.

Even as it orchestrates a military, political and media campaign aiming to intimidate China and whip up public support for military action in the Far East, the Obama administration wishes to preserve its ability to maneuver diplomatically and extract concessions from Beijing through political and diplomatic pressure.

The announcement that discussion on cyberwarfare will be central to the upcoming meeting between US and Chinese officials on "Economic and Strategic Dialogues" indicates that the issue is being used to bully China.

In April, the US Defense Department issued a report claiming that China launched a wave of hacks against US military information networks during 2014.

It cannot go unremarked that the hysterical condemnations of alleged Chinese cyberattacks by the US establishment have been steadily escalated even as the US has developed massive data mining operations against the Chinese government and military.

NSA internal documents leaked by whistleblower Edward Snowden showed that the spy agency has implanted "persistent" forms of malware technology on Chinese servers. Once embedded, the advanced malware technology used by the NSA can remain concealed indefinitely while transmitting data back to its controllers, performing manipulations of infected systems, and replicating itself on other networked computers.

There is little doubt that China conducts cyberespionage against the US government and military. But such efforts are dwarfed by the massive resources employed by the Pentagon, CIA and other US government agencies.

This week's events make clear that the alleged hacking will provide occasion for expanded use of similar technologies within the US. In response to supposed cyberthreats, the NSA demanded authority this week to conduct warrantless electronic surveillance against US-based Internet users and networks.

Previously, the National Security Agency has technically only enjoyed legal authorization to conduct dragnet electronic surveillance against servers and networks located overseas, despite the fact that the distinction between "overseas data" and "US data" has been rendered largely meaningless by the globalization of production and the revolution in communications and information technology that has unfolded since the 1970s.