US uses hacking allegations to escalate threats against China

Barry Grey
21 February 2013

The Obama administration is utilizing unsubstantiated charges of Chinese government cyber-attacks to escalate its threats against China. The past two days have seen allegations of hacking into US corporate and government web sites, hyped by the US media without any examination of their validity, employed to disorient the American public and justify an expansion of the Obama administration's drive to isolate China and prepare for an eventual military attack.

The accusations of hacking against China will also be used to justify increased domestic surveillance of computer and Internet communications, as well as an expanded use of cyber warfare methods internationally.

The *New York Times*, functioning once again as a conduit for the Pentagon and the CIA, has taken the lead in the latest provocation against Beijing. On Tuesday it published a bellicose front-page article headlined "China's Army Seen as Tied to Hacking Against US," and carrying the ominous subhead "Power Grid is a Target."

The article drips with cynicism and hypocrisy. It is well known that the United States is the world's most ruthless practitioner of cyber warfare. The article itself acknowledged that the US worked with Israel to disrupt the Iranian nuclear program by introducing the Stuxnet virus into Iran's computer systems. That bit of sabotage—itself an illegal act of aggression—was accompanied by a series of assassinations of Iranian scientists carried out by Israel with Washington's support.

The sprawling front-page article, which continued on an entire inside page of the newspaper, was based on a 60-page report released that day by a private computer security firm with close ties to the *Times*, as well as to the US military and intelligence agencies. The report by Mandiant—founded by a retired Air Force officer and based in Alexandria, Virginia—provides no real evidence to substantiate its claim that a unit of China's People's Liberation Army based in Shanghai is directing hacking attacks on US corporations, organizations and government institutions.

In its report, Mandiant claims to have tracked 141 cyber attacks by the same Chinese hacker group since 2006, 115 of which targeted US corporations. On the basis of Internet footprints, including Internet provider addresses, Mandiant concludes that 90 percent of the hacking attacks come from the same neighborhood in Shanghai. It then notes that the headquarters of Unit 61398 of the People's Liberation Army is located in that neighborhood. From this coincidence, Mandiant draws the entirely unwarranted inference that the cyber-attacks are coming from the PLA building.

As the *Times* admits in its article, "The firm was not able to place the hackers inside the 12-story [PLA Unit 61398 headquarters] building…" The newspaper goes on to report that "Mandiant also discovered an internal China Telecom memo discussing the state-owned telecom company's decision to install high-speed fiber-optic lines for Unit 61398's headquarters." One can only assume that Mandiant "discovered" this memo by carrying out its own hacking of Chinese computers.

Chinese spokesmen have denied any involvement by the government or the military in hacking attacks and dismissed the Mandiant report as lacking any proof of its charges. The Chinese Ministry of Defense released a statement Wednesday pointing out that Internet provider addresses do not provide a reliable indication of the origin of hacking attacks, since hackers routinely usurp IP addresses. A Foreign Ministry spokesman pointed out that China is constantly being targeted by hackers, most of which originate in the US.

The Chinese position was echoed by Dell Secureworks cyber-security expert Joe Stewart, who told the *Christian Science Monitor*: "We still don't have any hard proof that

[the hacker group] is coming out of that [PLA Unit 61398's] building, other than a lot of weird coincidence pointing in that direction. To me, it's not hard evidence."

The Obama administration followed up the *Times* article, which sparked a wave of frenzied media reports of Chinese cyber-attacks, by announcing on Wednesday that it would step up diplomatic pressure and consider more punitive laws to counter what it described as a wave of trade secret theft by China and other countries. The Associated Press reported that the administration was discussing "fines, penalties and tougher trade restrictions" directed against China.

The latest propaganda attack points to an escalation of the US offensive against China that went by the name "pivot to Asia" in Obama's first term. That policy included whipping up territorial disputes in the East China and South China seas between China and a series of countries in East Asia, including Japan, Vietnam and the Philippines.

It has also included the establishment of closer military ties and new US installations in a number of countries, including India and Australia, to militarily encircle China.

The *Times* concluded its article by reporting that "The mounting evidence of state sponsorship… and the growing threat to American infrastructure are leading officials to conclude that a far stronger response is necessary." It cited Rep. Mike Rogers, the Republican chairman of the House Intelligence Committee, as saying that Washington must "create a high price" to force the Chinese to back down.

In an editorial published Wednesday, the *Times* noted that the administration has decided to give US Internet providers and anti-virus vendors information on the signatures of Chinese hacker groups, leading to a denial of access to US networks for these groups. It also reported that President Obama last week signed an executive order authorizing increased sharing of information on cyber threats between the government and private companies that oversee critical infrastructure, such as the electrical grid.

The *Wall Street Journal* in its editorial called for "targeted sanctions" against Chinese individuals and institutions.

The background to this new salvo of anti-China propaganda underscores that it is part of an aggressive expansion of US military capabilities, both conventional and cyber-based. Obama raised the issue of cyber war in his February 12 State of the Union address, accusing US "enemies" of seeking to "sabotage our power grid, our financial institutions, our air traffic control systems," and insisting that action be taken against such attacks.

In the same speech, he defended his drone assassination program, which is based on the claim that the president has the unlimited and unilateral power to order the murder of anyone anywhere in the world, including US citizens.

Last October, Obama signed an executive order expanding military authority to carry out cyber-attacks and redefine as "defensive" actions that would previously have been considered acts of aggression—such as the cutting off of computer networks. Around the same time, Defense Secretary Leon Panetta gave a bellicose speech in which he warned of a "cyber Pearl Harbor." Panetta told *Time* magazine: "The three potential adversaries out there that are developing the greatest capabilities are Russia, China and Iran."

At the end of January, the *New York Times* accused Chinese authorities of hacking into its news operations, a charge that was quickly seconded by the *Washington Post* and the *Wall Street Journal*. That same week, the *Washington Post* reported that the US military had approved a five-fold increase of personnel in its Cyber Command. Days later, the *Times* reported on its front page that the Obama administration had concluded that the president had the power to authorize pre-emptive cyber war attacks.

This bellicose posture toward China and expansion of cyber warfare methods goes hand in hand with growing threats to democratic rights at home. The cyber war plans include options for military action within the US. The *Times* reported earlier this month that the military "would become involved in cases of a major cyber-attack within the United States" under certain vaguely defined conditions.

Efforts to increase government control of the Internet and surveillance of Internet communications are being stepped up. Just last week, Rep. Rogers of Michigan and Democratic Congressman Dutch Ruppersberger of Maryland reintroduced the Cyber Intelligence Sharing and Protection Act (CISPA). The bill died in the Senate last year in the midst of protests over provisions allowing the government to spy on emails and other Internet-based communications.