World Socialist Web Site wsws.org

Washington’s hacking charges escalate pressure on China

Alex Lantier
21 May 2013

Yesterday, top US officials and media outlets made unsubstantiated allegations of hacking of US computer systems by a military unit in Shanghai, escalating tensions with China.

The *New York Times* led this campaign, publishing an article titled “Chinese Hackers Resume Attacks on US Targets,” which served as a conduit for accusations and threats against China by US computer security firm Mandiant and US officials. The *Times* claimed that the Chinese army’s Unit 61398 in Shanghai, whose existence Washington alleged this February, “is back in business.”

The *Times* effectively admitted that it had no evidence to support its allegations. “It is not clear,” it wrote, “precisely who has been affected by the latest attacks. Mandiant, a private security company that helps companies and government agencies defend themselves from hackers, said the attacks had resumed but would not identify the targets, citing agreements with its clients.”

The *Times* claimed that China had targeted several firms—including Coca-Cola, French energy firm Schneider Electric, and US defense contractor Lockheed Martin—in previous attacks. None of these firms confirmed the *Times* ’ allegations, however, instead declining to comment.

This complete lack of evidence notwithstanding, current and former Obama administration officials speaking to the *Times* unleashed a torrent of threats against China. An unnamed US “senior official” said, “This is something we are going to have to come back at time and again with the Chinese leadership.” He added that Beijing has “to be convinced there is a real cost to this kind of activity.”

On Wednesday, former Obama administration Director of National Intelligence Dennis Blair and Ambassador to China John Huntsman are slated to release a plan for a series of executive orders and legislative acts to threaten China over the issue of hacking. Blair told the *Times*: “Jawboning alone won’t work. Something has to change in China’s calculus.”

The Obama administration mooted similar plans last month in a *Wall Street Journal* article, that described a “potentially rapid escalation” of tensions with China. According to the *Journal*, Washington is considering imposing “trade sanctions, diplomatic pressure, indictments of Chinese nationals in US courts and cyber countermeasures—both attack and defense.”

These unsubstantiated US accusations against Beijing over hacking drip with cynicism and hypocrisy. The US itself maintains the largest and most destructive cyber warfare apparatus in the world. It announced this March the formation of 13 offensive cyber war teams, writing malicious computer code to disable or destroy computers or computerized infrastructure, part of a multi-billion-dollar US cyber war program.

The Obama administration already claimed the right this February to wage pre-emptive cyber-attacks, transposing onto the Internet the illegal methods of aggression most infamously used by the Bush administration against Iraq. This came after the US and Israel worked together to disable Iran’s nuclear program by putting the Stuxnet virus into Iranian computer systems running nuclear centrifuges. This was accompanied by a series of bombings and assassinations inside Iran, targeting Iranian scientists.

Significantly, as elements of the US foreign policy establishment have admitted, what is driving Washington’s vague accusations of Chinese cyberwarfare is not primarily whatever hacking may be occurring, but the rising military tensions between the United States and China.

As Richard Falkenrath of the US Council on Foreign Relations said in February, describing US accusations of Chinese cyberwar hacking, "While this is all described in neutral terms—what are we going to do about cyber-attacks—the underlying question is, 'What are we going to do about China?'"

Military and diplomatic relations between the world's two largest economies have worsened dramatically since Washington's aggressive "pivot to Asia," aimed at containing China, announced during Obama's first term. Last month, Washington escalated military exercises with South Korea into a full-blown war scare with neighboring North Korea. It demonstratively deployed nuclear-capable B-2 Stealth bombers to the Korean peninsula, only a few hundred kilometers from China.

Cyber warfare looms large as an issue in US-China military relations, as electronic communications become ever more central to coordinating far-flung military forces, detecting them, and targeting them with precision-guided munitions. Such forces include not only traditional ones like US naval task forces built around aircraft carriers and troop transports, but also newer weapons such as US or Chinese remote-controlled or computer-operated drones.

Last week, the US Navy tested the X-47B—its first fully autonomous, computer-guided drone aircraft—on the aircraft carrier USS George H.W. Bush. The *Times* noted that "to offset China's numerical advantage and technological advances, the US Navy is betting heavily on drones—not just the X-47B and its successors, but anti-submarine reconnaissance drones, long-range communications drones, even underwater drones."

The paper noted the rising risk of accidental conflict, as the US fills the Pacific Ocean with "thousands" of drones, and China deploys its own drones so as not to fall too far behind.

The issue of cyber warfare is closely bound up with the accelerating arms race in the Pacific. The Pentagon's recent report to the US Congress on Chinese military capabilities stressed the role of Chinese cyber warfare planning as part of broader plans to deter a possible US intervention against China. One can only suppose that US preparations for cyber warfare against China are similarly or even more advanced.

The Pentagon wrote that China's "sustained investment" in cyberwarfare, guided missile, and space warfare capabilities "appear" designed to enable anti-access/area-denial missions (what PLA [Chinese People's Liberation Army] strategists refer to as 'counter-intervention operations'). … China continues to develop measures to deter or counter third-party intervention, particularly by the United States. China's approach to dealing with this problem is manifested in a sustained effort to develop the capability to attack at long ranges military forces that might deploy or operate within the Western Pacific."

The combination of US threats and unsubstantiated accusations and preparations, both Chinese and American, for what would be a cataclysmic Sino-American conflict, point to the profound crisis of world capitalism.

The industrial infrastructure underlying US-China trade, which totals one-half trillion dollars per year, is at the heart of the world economy. Yet under capitalism and the nation-state system, it must base itself on international financial and military relations which are now in an advanced state of collapse.

On the one hand, crisis-ridden American banks have accumulated trillions of dollars of debts to China, which they are ever less inclined to repay. On the other, while China's industrial growth has not pulled the Chinese working masses out of poverty, it has shaken US imperialism's geo-strategic hegemony, which underlay international relations in post-war Asia.

What is emerging is, as the great Russian Marxist Leon Trotsky wrote in 1914 at the beginning of World War I, the "revolt of the forces of production against the political form of nation and state." Then as now, the critical task is mobilizing the working class in a common international struggle for socialism and against imperialist war.