Washington steps up hacking allegations against China

Niles Williamson
29 May 2013

On Monday the *Washington Post* published a classified list compiled by the Pentagon's Defense Science Board of military systems and technologies allegedly compromised by Chinese hacking. Though the previously undisclosed report does not present any evidence for these claims, it is being used to escalate charges against China that it is hacking US secrets.

The allegations expanded on accusations published earlier this month that the Chinese government and its military, the People's Liberation Army (PLA), were engaged in a campaign of cyber-espionage against the United States. (See: "Washington's hacking charges escalate pressure on China")

The *Washington Post* 's report suggested that the Chinese government was utilizing cyber-espionage to steal information from military contractors in order to modernize its military and overcome the United States' military advantage. Defense contractors whose military systems have apparently been breached include Boeing, Lockheed Martin, Raytheon, and Northrop Grumman.

Amongst the compromised defense systems and technologies are the Patriot missile system, THAAD (Terminal High Altitude Area Defense, a system designed to shoot down ballistic missiles), and the Navy's Aegis ballistic-missile defense system. Key combat aircraft and ships including the F-35 fighter jet, Global Hawk surveillance drone, and the Navy's new Littoral combat ship are also included on the list. Purportedly compromised technologies include drone video and electronic warfare systems.

Oddly, while the Pentagon is claiming the Chinese hackers have compromised many of the American military's most advanced and sensitive weapons systems, it is not alleging that any designs have been stolen. Nor does it provide any substantial evidence as to the extent or timing of the supposed compromise of military defense designs. As such, it remains unclear as to how exactly this information has been compromised.

Some reports suggest that unidentified hackers may have targeted smaller subcontractors working for major US defense contractors. The 2013 National Defense Authorization Act (NDAA) requires defense contractors that hold classified clearance to report breaches of their networks and allow government investigators access to analyze the attacks. Attempts to require companies to secure their computer networks or lose Pentagon contracts failed last year, however.

This week's allegations against China build on unsubstantiated reports released earlier this month that the Chinese government and the PLA have engaged in direct cyber-attacks against the United States government and its military contractors. Cyber-attacks are notoriously difficult to trace, however, as it is easy for a hacker to launch an attack from another computer that he has taken over.

The Chinese government insists that it does not engage in cyber-espionage against the United States and often raises complaints that US targets China for cyber-attacks.

The US government's allegations against the Chinese government and PLA reek of hypocrisy. It is well established that the United States has engaged in its own systematic campaign of cyber-sabotage.

As part of Operation Olympic Games, the United States and Israel created the Stuxnet computer worm to attack Iran's nuclear facilities. The cyber-war operation was created under former President George W. Bush and expanded under President Obama. The Stuxnet worm caused centrifuges at the Natanz nuclear facility to destroy themselves by spinning out of control, temporarily setting back Iran's nuclear program. This campaign of cyber-sabotage occurred in conjunction with a US-backed assassination campaign carried out inside Iran against Iranian nuclear scientists.

The Pentagon is raising concerns about cyber-espionage and cyber-war as the United States escalates its moves to contain China as part of the Obama administration’s “pivot to Asia,” and its bid to maintain US geo-strategic hegemony worldwide. China has emerged as a major obstacle to US ambitions of enforcing economic hegemony in the Middle East. China, along with Russia, has repeatedly blocked UN Security Council votes that would have allowed direct intervention into the war in Syria.

Charges of cyber-espionage aim to place pressure on the newly instated regime of President Xi Jinping to get the Chinese government to shift its foreign policy broadly in line with US interests.

There are concerns that cyber-espionage by the PLA will undermine Washington’s technological advantage, should it start a war with China. The Pentagon also fears that China could use cyber-attacks to disrupt the critical communication networks the military relies on to coordinate and engage in attacks across the globe. According to the *Washington Post*, this threatens catastrophic results, including severed communication links critical to the operation of U.S. forces. Data corruption could misdirect U.S. operations. Weapons could fail to operate as intended. Planes, satellites or drones could crash.”

In tandem with the *Washington Post* ’s report, Australia’s ABC reported that the Australian government has also been subject to apparent Chinese cyber-attacks.

ABC reported that the plans for the Australian Security Intelligence Organization’s new $608 million headquarters were stolen in a cyber-attack on a building contractor. Security experts feared that China might use the blueprints to bug the building, which is currently under construction in the Australian capital of Canberra.

This case is a further example of the unreliability of cyber-espionage allegations, however, as the allegations were repudiated by the Australian government. Australia officials described the ABC report as unsubstantiated and Prime Minister Julia Gillard said that the report was “inaccurate.”

Chinese Foreign Ministry spokesman Hong Lei responded skeptically to the unsubstantiated allegations, saying, “Since it is technically untraceable, it is very difficult to find the source and identify the hacker. Therefore we have no idea what is the evidence for their report in which they make the claim with such certainty. Groundless accusations won’t solve the problem.”

The Pentagon’s accusations regarding Chinese cyber-espionage come ahead of the first meeting between President Obama and Chinese President Xi Jinping scheduled for June 7- 8 at the Annenberg Retreat in Rancho Mirage, California. Billed as a casual “get-to-know-you” retreat, it will be the first meeting between the two leaders since Xi became President in March. According to White House spokesman Jay Carney, Obama plans to raise the issue of cyber security with President Xi during the retreat.