# US preparations for cyber war against China

**Peter Symonds**
**23 February 2013**

The Obama administration, working hand-in-hand with the American media, has opened up a new front in its aggressive campaign against China. A slew of articles, most notably in the *New York Times*, has appeared over the past week purportedly exposing the involvement of the Chinese military in hacking US corporations and hinting at the menace of cyber warfare to vital American infrastructure such as the electricity grid.

The *Times* article on Tuesday based itself on the unsubstantiated and self-serving claims of a report prepared by cyber-security company Mandiant alleging that a Chinese military unit based in Shanghai had been responsible for sophisticated cyber-attacks in the US. (See: "US uses hacking allegations to escalate threats against China"). The rest of the media in the US and internationally followed suit, with articles replete with comments from analysts, think tanks and administration officials past and present about the "Chinese cyber threat", all but ignoring the emphatic denials by China's foreign and defence ministries.

This set the stage for the release on Wednesday of Obama's "Administration Strategy on Mitigation of Theft of US Trade Secrets," which, while not formally naming China, cited numerous examples of alleged Chinese cyber espionage. In broad terms, the document laid out the US response, including "sustained and coordinated diplomatic pressure" on offending countries and the implied threat of economic retaliation via "trade policy tools."

US Attorney General Eric Holder warned of "a significant and steadily increasing threat to America's economy and national security interests." Deputy Secretary of State Robert Hormats declared that the US had "repeatedly raised our concerns about trade secret theft by any means at the highest levels with senior Chinese officials."

The demonisation of China as a global cyber threat follows a well-established modus operandi: it is aimed at whipping up a public climate of fear and hysteria in preparation for new acts of aggression—this time in the sphere of cyber warfare. Since coming to office in 2009, Obama has launched a broad economic and strategic offensive aimed at weakening and isolating China and reinforcing US global dominance, especially in Asia.

Accusations of Chinese cyber theft dovetail with the Obama administration's economic thrust into Asia through its Trans Pacific Partnership (TPP)—a new multilateral trade agreement aimed at boosting US trade at China's expense. The protection of "intellectual property rights" is a central component of the TPP, as the profits of American corporations rest heavily on their monopoly over markets via brand names and technology. Allegations of cyber espionage will become the pretext for new trade war measures against China.

However, the more sinister aspect of the anti-Chinese propaganda is the US preparation of war against China. Under the banner of its "pivot to Asia," the Obama administration has put in train a far-reaching diplomatic and strategic offensive aimed at strengthening existing military alliances with Japan, South Korea, Australia, the Philippines and Thailand, forging closer strategic partnerships and ties, especially with India and Vietnam, and undermining close Chinese relations with countries like Burma and Sri Lanka.

Obama's "pivot to Asia" has already resulted in a dangerous escalation of maritime disputes in the South China Sea and East China Sea as Japan, the Philippines and Vietnam, encouraged by the US, have pressed their territorial claims against China. The focus on these strategic waters is not accidental, as they encompass the shipping lanes on which China relies to import raw materials and energy from the Middle East and Africa. The US is establishing new military basing

arrangements in Australia, South East Asia and elsewhere in the region to ensure it has the ability to choke off China's vital supplies in the event of a confrontation or war.

The Pentagon regards cyber warfare as a vital component of the huge American war machine and has devoted considerable resources towards its development, especially under the Obama administration. In May 2010, the Pentagon set up its new US Cyber Command headed by General Keith Alexander, director of the National Security Agency (NSA), drawing on the already massive cyber resources of the NSA and the American military.

US accusations of Chinese cyber espionage are utterly hypocritical. The NSA, among other US agencies, has been engaged in electronic spying and hacking into foreign computer systems and networks around the world on a vast scale. Undoubtedly, China is at the top of the list of prime targets. The Chinese Foreign Ministry claimed this week that at least 14 million computers in China were hacked by 73,000 overseas-based users last year, including many cyber attacks on the Chinese Defence Ministry.

The US has already engaged in aggressive, illegal acts of cyber sabotage against Iran's nuclear facilities and infrastructure. Together with Israel, it infected the electronic controllers of the gas centrifuges used in Iran's Natanz uranium enrichment plant with the Stuxnet worm, causing hundreds to spin out of control and self-destruct. This criminal activity took place alongside more traditional forms—the assassination of Iranian nuclear scientists and other acts of sabotage by Israel.

It is inconceivable that the Pentagon's cyber capacities are being deployed for purely defensive purposes against the "Chinese threat." Indeed, in taking over as cyber warfare chief in 2010, General Alexander outlined his credo to the House Armed Services subcommittee. After declaring that China was viewed as responsible for "a great many attacks on Western infrastructure," he added that if the US were subject to an organised attack, "I would want to go and take down the source of those attacks."

Last August, the US Air Force issued what was described by the *New York Times* as "a bluntly worded solicitation for papers advising it on 'cyberspace warfare attack capabilities,' including weapons to 'destroy, deny, deceive, corrupt or usurp' an enemy's computer networks and other hi-tech targets. The same article referred to the Pentagon's research arm, the Defence Advanced Research Projects Agency, hosting a gathering of private contractors wanting to participate in "Plan X"—the development of "revolutionary technologies for understanding, planning and managing cyber warfare."

This week's propaganda about the "Chinese cyber threat" provides the justifications for stepping up the already advanced US preparations for conducting cyber-attacks on Chinese military and civilian targets. Amid the rising tensions between the US and China produced by Obama's "pivot to Asia", reckless American actions in the sphere of cyber warfare only compound the danger of open military confrontation between the two powers.