Written by **William F. Jasper** on April 16, 2011

China Accelerates Cyber Attacks, Espionage

China's massive human rights violations, however, are a continuing reminder that the Communist-ruled "Middle Kingdom" is far from attaining the reformed status that is often wrongly bestowed upon it by journalists, politicians, and business leaders eager to exploit the China market. Another reminder comes in the form of China's aggressive espionage and cyber attacks.

A new report by the Reuters news agency says China has stepped up its cyber warfare against the United States and notes that in the electronic spy vs. spy conflict, "many experts believe China may have gained the upper hand."

Documents released by WikiLeaks and interviews with security experts "suggest that when it comes to cyber-espionage, China has leaped ahead of the United States," says the Reuters report. The Reuters story notes:

> According to U.S. investigators, China has stolen terabytes of sensitive data — from usernames and passwords for State Department computers to designs for multi-billion dollar weapons systems. And Chinese hackers show no signs of letting up. "The attacks coming out of China are not only continuing, they are accelerating," says Alan Paller, director of research at information-security training group SANS Institute in Washington, DC.

"Byzantine Hades"

The Reuters article reports:

> Secret U.S. State Department cables, obtained by WikiLeaks and made available to Reuters by a third party, trace systems breaches — colorfully code-named "Byzantine Hades" by U.S. investigators — to the Chinese military. An April 2009 cable even pinpoints the attacks to a specific unit of China's People's Liberation Army.

The unit that the attacks were traced to is the Chengdu Province First Technical Reconnaissance Bureau, an electronic espionage unit of the People's Liberation Army (PLA). "Much of the intrusion activity traced to Chengdu is similar in tactics, techniques and procedures to (Byzantine Hades) activity attributed to other" electronic spying units of the PLA, a State Department cable says.

The Technical Reconnaissance Bureaus, or TRBs, fall under the direction of the PLA's Third Department, which oversees electronic espionage. The TRBs are believed to be responsible for many of the tens of thousands of breaches of government and private computer systems that occur each year. Some of these cyber attacks — with code names such as Titan Rain, Aurora, and Night Dragon — have received relatively high-profile news coverage. However, the extensiveness and gravity of the breaches may be far greater than has been publicly admitted. Public officials and military leaders know there is a political cost and career cost to admissions of serious security failures, and corporate leaders know

there is a significant threat to consumer confidence — and ultimately a bottom-line impact — if customer data has been compromised.

There has also been a disturbing tendency on the part of politicians, officials, and academics who toe the Beijing Lobby line to minimize the extent and impact of the PRC's cyber warfare. It is common in many reports for "experts" to suggest that many of the attacks emanating from China may be the work of independent actors taking advantage of the country's "vulnerable computer infrastructure." The Beijing regime is only too willing to encourage this narrative of China-as-victim, which provides convenient deniability.

This is the line taken, for instance, by James A. Lewis of the Center for Strategic and International Studies at a 2005 CSIS program on China and cyber security. According to Lewis' presentation on "Computer Espionage, Titan Rain and China":

> China is particularly susceptible to being used as a platform for third country attacks because its networks are so vulnerable. Hackers can take over poorly secured Chinese computers and use them for criminal purposes without their owners' knowledge.

Lewis says that "an attack that can be traced back to China demonstrates little about the source. China is also the threat du jour. In the 1980s, Americans looked under their beds and believed they saw the KGB; now they believe they see the PLA." According to the school of thought subscribed to by Dr. Lewis, those who see the PLA's hand in cyber attacks coming out of China are suffering from paranoia. However, his shop-worn liberal trope about supposedly irrational fears of the KGB under the beds should have been laid to rest long ago by all thinking people. Dr. Lewis apparently doesn't know about the infamous penetrations of the CIA, FBI, and the Defense Department by Aldrich Ames, Robert Hannsen, and the Walker family spy ring.

And he would seem to be unaware of the vast body of evidence that has come out of the Venona documents and the Soviet archives showing that the KGB's penetration of American institutions was more than sufficient to vindicate the "paranoia" of the American right and to thoroughly discredit the "witch hunt" charges of the American left.

The arrests in the past months of Russian and Chinese spies in the United States (see here and here) provide ample evidence that the communist propensity for espionage and deception has not abated among the supposedly "reformed" leadership of the Beijing regime.

China's Worldwide Attacks

In addition to the U.S. Defense Department and major software, Internet, and energy companies, Chinese hackers have been implicated in cyber attacks on government institutions in Britain, India (see here and here), Australia, and dozens of other countries. Earlier this year the computers of Australian Prime Minister Julia Gillard and other government ministers and members of Parliament were compromised by China-based cyber spies. The *Daily Telegraph* reported on March 29 ("China spies suspected of hacking Julia Gillard's emails"):

> The parliamentary computers of at least 10 federal ministers including the Prime Minister, Foreign Minister and Defense Minister are suspected of being hacked into in a major breach of national security.

Among the ministers' parliamentary computers believed to have been compromised in Canberra were Foreign Minister Kevin Rudd and Defence Minister Stephen Smith.

> It is believed Prime Minister Julia Gillard's parliamentary computer was another compromised.

In February, McAfee, the computer security giant, published a report on the massive 2009 cyber attack known as "Night Dragon." The McAfee report states:

> Starting in November 2009, coordinated covert and targeted cyberattacks have been conducted against global oil, energy, and petrochemical companies. These attacks have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of remote administration tools (RATs) in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations. We have identified the tools, techniques, and network activities used in these continuing attacks-which we have dubbed Night Dragon-as originating primarily in China.

The report goes on to note:

> Attackers using several locations in China have leveraged C&C servers on purchased hosted services in the United States and compromised servers in the Netherlands to wage attacks against global oil, gas, and petrochemical companies, as well as individuals and executives in Kazakhstan, Taiwan, Greece, and the United States to acquire proprietary and highly confidential information. The primary operational technique used by the attackers comprised a variety of hacker tools, including privately developed and customized RAT tools that provided complete remote administration capabilities to the attacker. RATs provide functions similar to Citrix or Microsoft Windows Terminal Services, allowing a remote individual to completely control the affected system.

Perhaps one of the most serious (publicly) known compromises of U.S. national security by China-based hackers concerns the penetration of the Defense Department's costliest project ever — and its most technologically advanced — the Pentagon's $300 billion Joint Strike Fighter, also known as the F-35 Lightning II.

The consequences of the loss or compromise of vital information on a primary defense system such as the F-35 are enormous. But no less significant are the compromises of our nation's energy grid by Chinese hackers.

A *Wall Street Journa*l article in 2009 reported:

> Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.
>
> The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.
>
> "The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."
>
> The espionage appeared pervasive across the U.S. and doesn't target a particular company or region, said a former Department of Homeland Security official. "There are intrusions, and they are growing," the former official said, referring to electrical systems.
>
> "There were a lot last year."

The U.S. Director of National Intelligence James Clapper, in testimony to the U.S. Senate has characterized China's ongoing cyber warfare as a "formidable concern."

He cited the incident of April, 8, 2010, when state-owned China Telecom advertised erroneous network routes that instructed "massive volumes" of Internet traffic to go through Chinese servers for 17 minutes.

"This incident affected traffic to and from US government and military sites, including sites for the Senate, the Army, the Navy, the Marine corps, the air force, and the office of the Secretary of Defense, as well as a number of Fortune 500 firms," he said.

The acceleration of China's cyber warfare should not come as a surprise; it was heralded as far back as 1999, when two of the PLA's senior colonels published a major paper entitled Unrestricted Warfare, which, reportedly, has been adopted as a primary theoretical manual guiding the PLA's program of "asymmetrical warfare" as it applies to conflict between China and the (currently, at least) militarily superior United States.

Photo: F-35 Lightning II

Related articles:

Chinese Spying in the United States

Communist Propaganda Song Performed at White House

Pianist with Communist Roots Plays at White House State Dinner

KGB/FSB: The “Game” Remains the Same

Russia, China Spies Belie “End of the Cold War”