Written by **Alex Newman** on July 11, 2014

Chinese Target Feds' Data; Kerry Vows More Military Cooperation

Chinese hackers, presumably working for the Communist dictatorship in Beijing, broke into sensitive U.S. government computer systems in March holding information on federal employees, the *New York Times* reported on July 9, citing senior U.S. officials. The attack appears to have specifically targeted files on U.S. government workers who have applied for top-secret security clearances, a number in the tens of thousands. The Obama administration, however, responded by promising even more "cooperation" with the ruthless regime ruling mainland China.

According to media reports about the hacking breach, the Chinese operatives gained access to some databases at the Office of Personnel Management, which keeps records on all employees of the U.S. government. When the breach was detected, the hackers were supposedly blocked from the network, federal officials told the *Times*. It was apparently unclear how deep into the systems the hackers were able to reach.

Reports suggested that they could have obtained sensitive information on security-clearance applications including details of applicants' foreign contacts, employment history, drug use, and more. The potential for abuse of that information — compromising even more U.S. government secrets by compromising employees with security clearances, for example — is vast and potentially extremely dangerous, according to analysts.

The Department of Homeland Security, which admitted the breach occurred when questioned, tried to downplay fears. A senior official cited by the *Times* said that at this point, the responsible agencies had not "identified any loss of personally identifiable information." Still, an "emergency response team" was put on the case to the "assess and mitigate any risks identified," the Homeland Security official told the newspaper. The attack was indeed traced to China, as countless other, similar hackings have been.

The day after the explosive story appeared on the front page of the *Times*, U.S. Secretary of State John Kerry was in Beijing meeting with top officials in the communist regime for the U.S.-China "Strategic and Economic Dialogue." However, instead of dealing with the ongoing Chinese espionage targeting Americans — the regime is fiendishly gathering sensitive U.S. military, economic, and political intelligence — Kerry promised more "cooperation" on everything from terror and law enforcement to military issues.

Apparently "cybersecurity" collaboration has been put on the backburner for now. The communist regime's "top diplomat," Yang Jiechi, though, said Beijing wanted more U.S.-China cooperation based on mutual "trust" and "respect." "China believes cyber-space should not become a tool to harm other countries' interests," Yang said, equating the regime he serves with the nation it rules. "China hopes

the U.S. side can create the conditions to carry out U.S.-China dialogue and cooperation on the Internet."

Indeed, aside from "cyber" issues, "cooperation" between the U.S. government and China's mass-murdering regime has reached unprecedented proportions under the Obama administration. Late last year, for the first time in history, Communist Chinese troops were admittedly on American soil for an "exchange" mission with U.S. forces. The shocking scheme came shortly after similar plots with Russian terror troops in Colorado. Before that, a Chinese general who threatened to nuke American cities even led a military delegation to Washington. More recently, the U.S. government and the regime in China announced a partnership to fight "global warming."

Asked about the latest intrusion while in Beijing for the summit, Kerry seemed to know little about it. "Apparently this story relates to an attempted intrusion that is still being investigated by the appropriate U.S. authorities," he said. "It does not appear to have compromised any sensitive material. And I'm not going to get into any of the specifics of that ongoing investigation, but we've been very clear for some time with our counterparts here that this is in larger terms an issue of concern."

The Chinese dictatorship, as usual, denied responsibility for the latest attack, the *Wall Street Journal* reported. "Some U.S. media and U.S. cybersecurity always smear China and create the theory that China is a cyberthreat, but they can't provide sufficient evidence of that," claimed the regime's "Foreign Ministry" spokesman, Hong Lei, during a daily press briefing, claiming the dictatorship opposes hacking. "We feel strongly that these kinds of reports and comments are irresponsible and not worth a comment or refuting."

Apologists for the Chinese regime also pointed out that the National Security Agency was recently exposed in leaks by former NSA contractor Edward Snowden compromising the communications of Beijing autocrats and some state-owned "companies" in China. The fact remains, however, that the Chinese dictatorship has little in the way of technology that was not stolen or surreptitiously acquired from the West. Plus, if the U.S. government is going to spy on anyone, the barbaric regime responsible for murdering more innocent people than any other entity in human history is probably a good place to start — especially considering the fact that one of its top generals threatened to nuke hundreds of U.S. cities.

Of course, the Chinese regime's massive intelligence-gathering apparatus aimed at the United States has been exposed repeatedly. Experts say that, in terms of manpower, it is the largest spying leviathan in the world. Already, the U.S. government admits that the designs for many of the military's most advanced weapons systems — missile defenses, ships, fighter planes, and more — have been compromised by the dictatorship's legions of hackers. Much of the most sensitive U.S. technology, though, was compromised with the assistance of former President Bill Clinton, as revealed in the infamous "Chinagate" scandal.

More recently, in May, the U.S. Department of Justice unveiled a largely for-show indictment against five officers in the autocracy's "People's Liberation Army" (PLA) for hacking into the computer systems of six U.S. firms to steal trade secrets and other information. "When a foreign nation uses military or intelligence resources and tools against an American executive or corporation to obtain trade secrets or sensitive business information for the benefit of its state-owned companies, we must say: Enough is enough," said Attorney General Eric Holder.

In reality, the chances of any of those hackers being held accountable are slim to none, and the regime

in Beijing knows it. At least two senior U.S. intelligence officials quoted by the *Times* alluded to the fact that with no real consequences for the Chinese dictatorship or even its lower-level operatives, the regime has little incentive to stop. In fact, instead of accountability, the Obama administration continues to reward the ruthless autocracy with more and more "cooperation" on everything from security to the economy. This week, it happened again, according to news reports.

In the latest attack, federal officials failed to publicly report the breach in the personnel systems, which stands in contrast to instructions the Obama administration has offered to private-sector entities. Obama spokesperson Caitlin Hayden, though, suggested this case was different. "The administration has never advocated that all intrusions be made public," she was quoted as saying. "We have advocated that businesses that have suffered an intrusion notify customers if the intruder had access to consumers' personal information. We have also advocated that companies and agencies voluntarily share information about intrusions."

In 2010, *The New American* magazine ran a major report on Chinese espionage operations against the United States. In addition to compromising much of America's military technology, the regime has also been wildly successful at stealing U.S. trade secrets, helping to boost its bloated and inefficient state-owned "companies" by letting private Western firms invest in the research and development. Beijing has also become notorious for spying on dissidents who have fled abroad to escape its communist tyranny.

While the U.S. government is pretending to be concerned about Chinese espionage, it has become clear that Washington's alleged "counterintelligence" efforts have been a joke at best — and a deceptive fraud at worst. The Obama administration should immediately stop *all* cooperation with the regime — especially in military, security, and economic scheming — and quit pretending that mass-murderers and megalomaniacs who enslaved over a billion people (with U.S. support) represent a legitimate government. Beijing is already demanding a "de-Americanized New World Order." If U.S. policy does not change, there should be little doubt that the regime will get its wish.

Alex Newman, a foreign correspondent for The New American*, is currently based in Europe. He can be reached at anewman@thenewamerican.com. Follow him on Twitter @ALEXNEWMAN_JOU.*

Related articles:

Chinese Spying in the United States

U.S. Accuses China of Spying; China Calls Charges Hypocritical

Communist Chinese Troops on U.S. Soil for "Exchange" Mission

In China, Tyranny Remains 25 Years After Tiananmen Massacre

China, G77 Tyrants, and UN Boss Demand "New World Order"

Communist Chinese Regime Steps up War on Churches

With Dollar Demise in Focus, Beijing Pushes "New World Order"

Hu Gets Red-carpet Treatment at White House

China Betrayed Into Communism

Communist Chinese Regime Forcing Rural Population Into Cities

George Soros Touts China as Leader of New World Order