The New York Times | http://nyti.ms/1h5uomv

WORLD | NYT NOW

U.S. Tries Candor to Assure China on Cyberattacks

By DAVID E. SANGER APRIL 6, 2014

WASHINGTON — In the months before Defense Secretary Chuck Hagel's arrival in Beijing on Monday, the Obama administration quietly held an extraordinary briefing for the Chinese military leadership on a subject officials have rarely discussed in public: the Pentagon's emerging doctrine for defending against cyberattacks against the United States — and for using its cybertechnology against adversaries, including the Chinese.

The idea was to allay Chinese concerns about plans to more than triple the number of American cyberwarriors to 6,000 by the end of 2016, a force that will include new teams the Pentagon plans to deploy to each military combatant command around the world. But the hope was to prompt the Chinese to give Washington a similar briefing about the many People's Liberation Army units that are believed to be behind the escalating attacks on American corporations and government networks.

So far, the Chinese have not reciprocated — a point Mr. Hagel plans to make in a speech at the P.L.A.'s National Defense University on Tuesday.

The effort, senior Pentagon officials say, is to head off what Mr. Hagel and his advisers fear is the growing possibility of a fast-escalating series of cyberattacks and counterattacks between the United States and China. This is a concern especially at a time of mounting tensions over China's expanding claims of control over what it argues are exclusive territories in the East and South China Seas, and over a new air defense zone. In interviews, American officials say their latest initiatives were inspired by Cold-War-era exchanges held with the Soviets so that each side understood the "red lines" for employing nuclear weapons against each other.

"Think of this in terms of the Cuban missile crisis," one senior Pentagon official said. While the United States "suffers attacks every day," he said, "the

last thing we would want to do is misinterpret an attack and escalate to a real conflict."

Mr. Hagel's concern is spurred by the fact that in the year since President Obama explicitly brought up the barrage of Chinese-origin attacks on the United States with his newly installed counterpart, President Xi Jinping, the pace of those attacks has increased. Most continue to be aimed at stealing technology and other intellectual property from Silicon Valley, military contractors and energy firms. Many are believed to be linked to cyberwarfare units of the People's Liberation Army acting on behalf of state-owned, or state-affiliated, Chinese companies.

"To the Chinese, this isn't first and foremost a military weapon, it's an economic weapon," said Laura Galante, a former Defense Intelligence Agency cyberspecialist. She now works for the Mandiant division of FireEye, one of the largest of the many cybersecurity firms seeking to neutralize attacks on corporations from China and other countries, as well as criminal groups and hackers.

Administration officials acknowledge that Mr. Hagel, on his first trip to China as defense secretary, has a very difficult case to make, far more complicated than last year. The Pentagon plans to spend $26 billion on cybertechnology over the next five years — much of it for defense of the military's networks, but billions for developing offensive weapons — and that sum does not include budgets for the intelligence community's efforts in more covert operations. It is one of the few areas, along with drones and Special Operations forces, that are getting more investment at a time of overall Pentagon cutbacks.

Moreover, disclosures about America's own focus on cyberweaponry — including American-led attacks on Iran's nuclear infrastructure and National Security Agency documents revealed in the trove taken by Edward J. Snowden, the former agency contractor — detail the degree to which the United States has engaged in what the intelligence world calls "cyberexploitation" of targets in China.

The revelation by The New York Times and the German magazine Der Spiegel that the United States has pierced the networks of Huawei, China's giant networking and telecommunications company, prompted Mr. Xi to raise the issue with Mr. Obama at a meeting in The Hague two weeks ago. The attack on Huawei, called Operation Shotgiant, was intended to determine whether the

company was a front for the army, but also focused on learning how to get inside Huawei's networks to conduct surveillance or cyberattacks against countries — Iran, Cuba, Pakistan and beyond — that buy the Chinese-made equipment. Other cyberattacks revealed in the documents focused on piercing China's major telecommunications companies and wireless networks, particularly those used by the Chinese leadership and its most sensitive military units.

Mr. Obama told the Chinese president that the United States, unlike China, did not use its technological powers to steal corporate data and give it to its own companies; its spying, one of Mr. Obama's aides later told reporters, is solely for "national security priorities." But to the Chinese, for whom national and economic security are one, that argument carries little weight.

"We clearly don't occupy the moral high ground that we once thought we did," said one senior administration official.

For that reason, the disclosures changed the discussion between the top officials at the Pentagon and the State Department and their Chinese counterparts in quiet meetings intended to work out what one official called "an understanding of rules of the road, norms of behavior," for China and the United States.

The decision to conduct a briefing for the Chinese on American military doctrine for the use of cyberweapons was a controversial one, not least because the Obama administration has almost never done that for the American public, though elements of the doctrine can be pieced together from statements by senior officials and a dense "Presidential Decision Directive" on such activities signed by Mr. Obama in 2012. (The White House released declassified excerpts at the time; Mr. Snowden released the whole document.)

Mr. Hagel alluded to the doctrine a week ago when he went to the retirement ceremony for Gen. Keith B. Alexander, the first military officer to jointly command the N.S.A. and the military's Cyber Command. General Alexander was succeeded last week by Adm. Michael S. Rogers, who as the head of the Navy's Fleet Cyber Command was a central player in developing a corps of experts who could conduct cyberwarfare alongside more traditional Navy forces.

"The United States does not seek to militarize cyberspace," Mr. Hagel said at the ceremony, held at the N.S.A.'s headquarters at Fort Meade, Md. He went on to describe a doctrine of "minimal use" of cyberweaponry against other

states. The statement was meant to assure other nations — not just China — that the United States would not routinely use its growing arsenal against them.

In Beijing, the defense secretary "is going to stress to the Chinese that we in the military are going to be as transparent as possible," said Rear Adm. John Kirby, the Pentagon press secretary, "and we want the same openness and transparency and restraint from them."

Experts here and in China point out that a lot was left out of Mr. Hagel's statement last week. The United States separates offensive operations of the kind that disabled roughly 1,000 centrifuges in Iran's nuclear program, America's best-known (and still unacknowledged) cyberattack against another state, from the far more common computer-enabled espionage of the kind carried out against the Chinese to gather information about a potential adversary.

"It's clear that cyberspace is already militarized, because we've seen countries using cyber for military purposes for 15 years," said James Lewis, an expert at the Center for Strategic and International Studies. "The Chinese have had offensive capabilities for years as well," he said, along with "more than a dozen countries that admit they are developing them."

A version of this article appears in print on April 7, 2014, on page A1 of the New York edition with the headline: U.S. Tries Candor to Assure China on Cyberattacks.