The New York Times | http://nyti.ms/1Kn0Ai8

ASIA PACIFIC

U.S. and China Seek Arms Deal for Cyberspace

点击查看本文中文版 | Read in Chinese

By **DAVID E. SANGER** SEPT. 19, 2015

WASHINGTON — The United States and China are negotiating what could become the first arms control accord for cyberspace, embracing a commitment by each country that it will not be the first to use cyberweapons to cripple the other's critical infrastructure during peacetime, according to officials involved in the talks.

While such an agreement could address attacks on power stations, banking systems, cellphone networks and hospitals, it would not, at least in its first version, protect against most of the attacks that China has been accused of conducting in the United States, including the widespread poaching of intellectual property and the theft of millions of government employees' personal data.

The negotiations have been conducted with urgency in recent weeks, with a goal to announce an agreement when President Xi Jinping of China arrives in Washington for a state visit on Thursday. President Obama hinted at the negotiations on Wednesday, when he told the Business Roundtable that the rising number of cyberattacks would "probably be one of the biggest topics" of the summit meeting, and that his goal was to see "if we and the Chinese are able to coalesce around a process for negotiations" that would ultimately "bring a lot of other countries along."

But a senior administration official involved in the discussions cautioned that an initial statement between Mr. Obama and Mr. Xi may not contain "a specific, detailed mention" of a prohibition on attacking critical infrastructure. Rather, it would be a more "generic embrace" of a code of conduct adopted recently by a working group at the United Nations.

One of the key principles of the United Nations document on principles for cyberspace is that no state should allow activity "that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." The goal of the American negotiators is to have Chinese leaders embrace the principles of the United Nations code of conduct in a bilateral agreement with Washington.

But it seems unlikely that any deal coming out of the talks would directly address the most urgent problems with cyberattacks of Chinese origin, according to officials who spoke on the condition of anonymity to describe continuing negotiations.

Most of those attacks have focused on espionage and theft of intellectual property. The rules under discussion would have done nothing to stop the theft of 22 million personal security files from the Office of Personnel Management, which the director of national intelligence, James R. Clapper Jr., recently told Congress did not constitute an "attack" because it was intelligence collection — something the United States does, too.

The agreement being negotiated would also not appear to cover the use of tools to steal intellectual property, as the Chinese military does often to bolster state-owned industries, according to an indictment of five officers of the People's Liberation Army last year. And it is not clear that the rules would prohibit the kind of attack carried out last year against Sony Pictures Entertainment, for which the United States blamed North Korea. That attack melted down about 70 percent of Sony's computer systems.

Sony is not, by most definitions, part of the nation's "critical infrastructure," although the Department of Homeland Security does

include “movie studios” on its list of critical “commercial facilities,” along with stadiums, museums and convention centers.

Still, any agreement to limit cyberattacks in peacetime would be a start. “It would be the first time that cyber is treated as a military capability that needs to be governed as nuclear, chemical and biological weapons are,” said Vikram Singh, a former Pentagon and State Department official who is now vice president for international security at the Center for American Progress.

Within the Obama administration, the effort to design “a set of norms of behavior” to limit cyberattacks has been compared to President John F. Kennedy’s first major nuclear treaty with the Soviet Union in 1963, which banned atmospheric nuclear tests. That accord did not stop the development of nuclear weapons or even halt underground tests, which continued for decades. But it was a first effort to prevent an environmental disaster, just as this would be a first effort by the world’s two biggest economic powers to prevent the most catastrophic use of cyberweapons.

Joseph S. Nye, a Harvard professor known for his studies of American power, said the concept of a “no first use” doctrine for cyberattacks had been “gestating for some time” in a variety of international forums. “It could create some self-restraint,” Mr. Nye said, but he added that the problem was, “how do you verify it, and what is its value if it can’t be verified?”

That problem goes to the heart of why arms control agreements in the cyberspace arena are so much more complicated than better-known agreements covering nuclear weapons.

In the Cold War and still today, nuclear arms remain in the hands of states, meaning they can usually be counted and their movements observed. Cyberweapons, too, are often developed by countries — the United States, Russia, China and Iran are among the most sophisticated — but they can also be found in the hands of criminal groups and teenagers, neither of which negotiate treaties.

Moreover, it was usually clear where a conventional attack had originated; the trajectory of a missile could be tracked by radar or satellite. Mr. Obama himself noted last week the difficulty of tracing a cyberattack, and thus of deterring it — or retaliating with confidence.

Earlier efforts to get Mr. Xi and other senior Chinese leaders to address cyberattacks have largely failed. Mr. Obama spent a considerable amount of time on the issue during a summit meeting with Mr. Xi at Sunnylands, a California estate, in 2013. But even after that session, the Chinese denied that their military was involved in attacks, and portrayed themselves as victims of attacks from the United States.

It was not an entirely spurious claim: Classified documents released by Edward J. Snowden showed a complex effort by the National Security Agency to get into the systems of a Chinese telecommunications giant, Huawei, though the United States maintained that the effort was for national security surveillance, not for the theft of intellectual property.

The recent Chinese movement on cybersecurity can be traced to several events, officials say.

The Office of Personnel Management breach, which went undetected for roughly a year, was traced to Chinese sources, and one official said evidence had been presented to Chinese officials. In August, Susan E. Rice, Mr. Obama's national security adviser, took a trip to Beijing to meet with Mr. Xi and other officials, and used it to increase pressure on China, suggesting that newly devised economic sanctions could be imposed. Mr. Obama referred to that possibility in two recent speeches, suggesting that he would hold off only if there was progress with Mr. Xi.

Last week, a high-level Communist Party envoy, Meng Jianzhu, who is responsible for state security, came to Washington and met with Ms. Rice, several American intelligence officials and the director of the F.B.I., James B. Comey. That session focused on coming up with some kind of agreement, however vaguely worded, that Mr. Obama and Mr. Xi could announce on Friday.

For the United States, agreements limiting cyberweapons are also problematic. The country is spending billions of dollars on new generations of weapons, and in at least one famous case, the cyberattacks on Iran's nuclear enrichment site at Natanz, it has used them.

American cyberwarriors would be concerned about any rules that limited their ability in peacetime to place "beacons" or "implants" in foreign computer networks; these are pieces of code that monitor how foreign computer systems work, and they can be vital in determining how to launch a covert or wartime attack. The Chinese have littered American networks with similar technology, often to the consternation of the Pentagon and intelligence agencies.

"One of the things to look for are any rules that bar 'preparing the battlefield,' " said Robert K. Knake, a senior fellow at the Council on Foreign Relations who worked in the White House cybersecurity office earlier in the Obama administration.

Mr. Obama, who has said little about the United States' development of cyberweapons during his presidency, has begun to talk about it in recent days. "If we wanted to go on offense, a whole bunch of countries would have some significant problems," he told the Business Roundtable on Wednesday.

A version of this article appears in print on September 20, 2015, on page A1 of the New York edition with the headline: U.S. and China Seek Arms Deal for Cyberspace.
