**Reports that Chinese Hackers have been probing infrastructure systems for at least five years is very disturbing. In the event that hostilities are initiated, they will doubtless attempt to disrupt our power stations and water infrastructure. We can assume that other adversaries like the Russians and N. Korea will also conduct this type of very disruptive activities to foment chaos.**

Given that our national security agencies have been aware of Chinese, and presumably probes by Russians and North Koreans, our security agencies involved with cryptology should already have been conducting similar actions against all our foes who either have the capability, or who have actually conducted, such operations. The ability to successfully disrupt any enemy’s infrastructure is essential to our national security and survival, therefore, we should believe that we have conducted similar probes to our foes. And, they must know that we can disrupt their infrastructure which is the ideal defense for deterring anyone who wants to use these techniques to seriously attack America.

This type of 21st Century warfare is highly classified, so until these techniques are revealed, we must just trust that our Cyber Warriors have been very busy probing the infrastructure of our potential foes, so that they know that they are also vulnerable, and the loss of power stations and water infrastructure will be very damaging to them as well.

These are not warfare strategies used by our past military leadership, so our current military leaders must not fall back to warfare tactics and strategies that were successful in the past. Warfare is no longer based on hardware, the best software will determine the winner of any major conflict.

**==============================================**

**Chinese hackers have lurked in some US infrastructure systems for ‘at least five years’**

**By Sean Lyngaas, *CNN*, February 7, 2024**

The Chinese hackers behind a campaign to infiltrate transportation hubs and other critical American infrastructure have had access to some of their targets’ computer networks for “at least five years,” according to a new report by US and allied security agencies obtained by CNN.

The campaign is part of a long-running effort by the hackers to position themselves for potentially crippling cyberattacks that could disrupt water and electricity, according to US officials.

US intelligence chiefs sounded the alarm about the threat to Congress last week, saying Beijing could use the hackers to disrupt a US response if China invades Taiwan. FBI Director Christopher Wray told lawmakers last week that the hackers could “wreak havoc and cause real-world harm” to the US.

The nearly 50-page report comes as US-China tensions over Taiwan and other key issues remain high and shows how central cyber operations could be to Chinese efforts to hobble US infrastructure in the event of a conflict between the two superpowers, according to US officials. The report would be the most detailed disclosure yet by the US government of the hackers’ stealthy techniques, one aimed at helping private owners of critical infrastructure spot the Chinese hackers in their networks.

The hackers’ presence in critical US networks has sparked a monthslong effort by US national security officials to kick the hackers out.

The report, which US officials are set to release this week, makes clear that the Chinese hackers’ activity began much earlier than previously known, with the hackers scoping and accessing IT systems years ago. From there, they have spent months looking for ways to maneuver onto more sensitive industrial systems that help control power flow and water.

The Beijing-backed hackers have been probing systems that control heating, cooling and water, access that, if exploited, could allow them to manipulate those systems and cause “significant infrastructure failures,” the report says. The hackers have also broken into security cameras at unnamed critical facilities, according to the document.

There are no signs yet that China has decided to use the hackers’ presence to disrupt US infrastructure, according to US officials, but they are concerned that could change quickly in the event of a crisis.

Liu Pengyu, a spokesperson for the Chinese Embassy in Washington, denied the US hacking allegations in a statement to CNN on Wednesday and accused Washington of conducting its own cyberattacks.

The new report also sheds new light on the sprawling nature of the hacking operation and on concerns from US allies over the activity.

US officials have confirmed the hackers have broken into computer networks at energy, transportation and water facilities in the “continental and non-continental” US and its overseas territories, including Guam, according to the report. In one case, after breaching the IT systems at an unnamed water facility, the hackers had access to a range of critical information on water treatment plants and water wells, according to the analysis.

The FBI, National Security Agency and Cybersecurity and Infrastructure Security Agency are among the US agencies that produced the report, along with cybersecurity agencies from Australia, Canada, New Zealand and the United Kingdom. CNN obtained a non-public version of the report, and sources familiar with the report told CNN the agencies are preparing to publish a version of it this week.

Canada’s cybersecurity agency “assesses that the direct threat to Canada’s critical infrastructure” from the Chinese hackers “is likely lower” than that to US infrastructure, but that Canada would still likely still be affected by a disruption to US infrastructure due to “cross-border integration,” the document says. Australia and New Zealand, two key allies in the US quest to counter China in the Pacific, could be vulnerable to similar activity from Chinese government hackers, the report says.