

The Washington Post

National Security

China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare

by [Ellen Nakashima](#) and [Paul Sonne](#) June 8 [✉Email the author](#)

Chinese government hackers have compromised the computers of a Navy contractor, stealing massive amounts of highly sensitive data related to undersea warfare — including secret plans to develop a supersonic anti-ship missile for use on U.S. submarines by 2020, according to American officials.

The breaches occurred in January and February, the officials said, speaking on the condition of anonymity to discuss an ongoing investigation. The hackers targeted a contractor who works for the Naval Undersea Warfare Center, a military organization headquartered in Newport, R.I., that conducts research and development for submarines and underwater weaponry.

The officials did not identify the contractor.

Taken were 614 gigabytes of material relating to a closely held project known as Sea Dragon, as well as signals and sensor data, submarine radio room information relating to cryptographic systems, and the Navy submarine development unit's electronic warfare library.

The Washington Post agreed to withhold certain details about the compromised missile project at the request of the Navy, which argued that their release could harm national security.

[China to U.S.: It's your fault we are in the South China Sea]

The data stolen was of a highly sensitive nature despite being housed on the contractor's unclassified network. The officials said the material, when aggregated, could be considered classified, a fact that raises concerns about the Navy's ability to oversee contractors tasked with developing cutting-edge weapons.

The breach is part of China's long-running effort to blunt the U.S. advantage in military technology and become the preeminent power in East Asia. The news comes as the Trump administration is seeking to secure Beijing's support in persuading North Korea to give up nuclear weapons, even as tensions persist between the United States and China over trade and defense matters.

The Navy is leading the investigation into the breach with the assistance of the FBI, officials said. The FBI declined to comment.

On Friday, the Pentagon inspector general's office said that Defense Secretary Jim Mattis had asked it to review contractor cybersecurity issues arising from The Post's story.

Cmdr. Bill Speaks, a Navy spokesman, said, "There are measures in place that require companies to notify the government when a 'cyber incident' has occurred that has actual or potential adverse effects on their networks that contain controlled unclassified information."

Speaks said that "it would be inappropriate to discuss further details at this time."

Altogether, details on hundreds of mechanical and software systems were compromised — a significant breach in a critical area of warfare that China has identified as a priority, both for building its own capabilities and challenging those of the United States.

"It's very disturbing," said former senator James M. Talent (R-Mo.), who is a member of the U.S.-China Economic and Security Review Commission. "But it's of a piece with what the Chinese have been doing. They are completely focused on getting advanced weapons technology through all kinds of means. That includes stealing secrets from our defense contractors." Talent had no independent knowledge of the breach.

Undersea priority

The Sea Dragon project is an initiative of a special Pentagon office stood up in 2012 to adapt existing U.S. military technologies to new applications. The Defense Department, citing classification levels, has released little information about Sea Dragon other than to say that it will introduce a “disruptive offensive capability” by “integrating an existing weapon system with an existing Navy platform.” The Pentagon has requested or used more than \$300 million for the project since late 2015 and has said it plans to start underwater testing by September.

Military experts fear that China has developed capabilities that could complicate the Navy’s ability to defend U.S. allies in Asia in the event of a conflict with China.

The Chinese are investing in a range of platforms, including quieter submarines armed with increasingly sophisticated weapons and new sensors, Adm. Philip S. Davidson said during his April nomination hearing to lead U.S. Indo-Pacific Command. And what they cannot develop on their own, they steal — often through cyberspace, he said.

“One of the main concerns that we have,” he told the Senate Armed Services Committee, “is cyber and penetration of the dot-com networks, exploiting technology from our defense contractors, in some instances.”

In February, Director of National Intelligence Daniel Coats testified that most of the detected Chinese cyber operations against U.S. industry focus on defense contractors or tech firms supporting government networks.

In recent years, the United States has been scrambling to develop new weapons or systems that can counter a Chinese naval buildup that has targeted perceived weaknesses in the U.S. fleet. Key to the American advantage in any faceoff with China on the high seas in Asia will be its submarine fleet.

“U.S. naval forces are going to have a really hard time operating in that area, except for submarines, because the Chinese don’t have a lot of anti-submarine warfare capability,” said Bryan Clark, a naval analyst at the Center for Strategic and Budgetary Assessments. “The idea is that we are going to rely heavily on submarines in the early effort of any conflict with the Chinese.”

China has made closing the gap in undersea warfare one of its three top military priorities, and although the United States still leads the field, China is making a concerted effort to diminish U.S. superiority.

“So anything that degrades our comparative advantage in undersea warfare is of extreme significance if we ever had to execute our war plans for dealing with China,” said James Stavridis, dean of the Fletcher School of Law and Diplomacy at Tufts University and a retired admiral who served as supreme allied commander at NATO.

The U.S. military let its anti-ship weaponry languish after the Cold War ended because with the Soviet Union’s collapse, the Navy no longer faced a peer competitor on the seas. But the rapid modernization and buildup of the Chinese navy in recent years, as well as Russia’s resurgent forces at sea, have prompted the Pentagon to renew heavy investment in technologies to sink enemy warships.

The introduction of a supersonic anti-ship missile on U.S. Navy submarines would make it more difficult for Chinese warships to maneuver. It also would augment a suite of other anti-ship weapons that the U.S. military has been developing in recent years.

Ongoing breaches

For years, Chinese government hackers have siphoned information on the U.S. military, underscoring the challenge the Pentagon faces in safeguarding details of its technological advances. Over the years, the Chinese have snatched designs for the F-35 Joint Strike Fighter; the advanced Patriot PAC-3 missile system; the Army system for shooting down ballistic missiles known as Terminal High Altitude Area Defense; and the Navy’s new Littoral Combat Ship, a small surface vessel designed for near-shore operations, according to previous reports prepared for the Pentagon.

In some cases, suspected Chinese breaches appear to have resulted in copycat technologies, such as the drones China has produced that mimic U.S. unmanned aircraft.

[Chinese cyberspies stole a long list of U.S. weapons designs]

Speaks, the Navy spokesman, said: “We treat the broader issue of cyber-intrusion against our contractors very seriously. If such an intrusion were to occur, the appropriate parties would be looking at the specific incident, taking measures to protect current information, and mitigating the impacts that might result from any information that might have been compromised.”

The Pentagon’s Damage Assessment Management Office has conducted an assessment of the damage, according to the U.S. officials. The Office of the Secretary of Defense declined to comment.

Theft of an electronic warfare library, Stavridis said, could give the Chinese “a reasonable idea of what level of knowledge we have about their specific [radar] platforms, electronically and potentially acoustically, and that deeply reduces our level of comfort if we were in a close undersea combat situation with China.”

Signals and sensor data is also valuable in that it presents China with the opportunity to “know when we would know at what distance we would be able to detect their submarines,” he said — again a key factor in undersea battles.

Investigators say the hack was carried out by the Chinese Ministry of State Security, a civilian spy agency responsible for counterintelligence, foreign intelligence and domestic political security. The hackers operated out of an MSS division in the province of Guangdong, which houses a major foreign hacking department.

Although the Chinese People’s Liberation Army is far better-known than the MSS when it comes to hacking, the latter’s personnel are more skilled and much better at hiding their tracks, said Peter Mattis, a former analyst in the CIA counterintelligence center. The MSS, he said, hacks for all forms of intelligence: foreign, military and commercial.

In September 2015, in a bid to avert economic sanctions, Chinese President Xi Jinping pledged to President Barack Obama that China would refrain from conducting commercial cyberespionage against the United States. Following the pact, China appeared to have curtailed much, although not all, of its hacking activity against U.S. firms, including by the People’s Liberation Army.

Both China and the United States consider spying on military technology to fall outside the pact. “The distinction we’ve always made is there’s a difference between conducting espionage in order to protect national security and conduct military operations, and the theft of intellectual property for the benefit of companies inside your country,” said Michael Daniel, the White House cybersecurity coordinator under Obama.

 **2113 Comments**

Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. She has also served as a Southeast Asia correspondent and covered the White House and Virginia state politics. She joined The Post in 1995.

 Follow @nakashimae

Paul Sonne covers the U.S. military and national security. He previously reported for the Wall Street Journal from Moscow, London and Washington.  Follow @PaulSonne

The Washington Post

The story must be told.

Your subscription supports journalism that matters.

Try 1 month for \$1

