What it will look like if China launches cyberattacks in the U.S.
Maggie Miller - Politico

While much of the cybersecurity world's attention is on fending off Russian hacks against Ukraine, American officials are increasingly worried about another growing threat: attacks by China on U.S. soil.

"If Xi Jinping moves on Taiwan, we should assume he'll launch cyberattacks against the United States as part of the operation," Rep. Mike Gallagher (R-Wis.), chair of the House Select Committee on China, said in an emailed statement.© Alex Brandon/AP Photo, file

If China invades Taiwan, they say, it is likely to unleash a volley of digital strikes against the United States at the same time.

Beijing continues to issue bold threats against the island. Most recently, China renewed military drills around the island in response to last week's meetings in the U.S. between Taiwan's president and House leaders — a meeting China called a "provocation."
Top lawmakers, the U.S. intelligence community and cybersecurity officials have warned in recent weeks that if an invasion happens, China would likely try to hobble critical U.S. systems with cyberattacks on military transport systems like ports and railroads, or against key civilian services like water and electricity.

"If Xi Jinping moves on Taiwan, we should assume he'll launch cyberattacks against the United States as part of the operation," Rep. Mike Gallagher (R-Wis.), chair of the House Select Committee on China, said in an emailed statement.
"This would likely include attacks on our electrical grid, water systems and communications infrastructure — especially near key military installations."

Chinese hackers could also attack the networks of companies that provide services to the military or to critical infrastructure operators, holding their systems hostage for ransom payments.

"If you get the right supply chain, it can have a lot of effects against a lot of targets," said John Hultquist, head of Mandiant Intelligence Analysis at Google Cloud.

China is viewed as one of the most dangerous nations in cyberspace, and its cyber espionage operations are among some of the U.S. government's top cyber-related investigations.

FBI Director Christopher Wray said in 2020 that his agency opens a new investigation into a Chinese counterintelligence effort every 10 hours, and half of the FBI's counterintelligence investigations are related to China. And the intelligence community's threats assessments have long warned that China is "almost certainly capable" of launching disruptive and destructive cyberattacks.

But China hasn't fully demonstrated its destructive cyber capabilities to the world when compared with Russia or Iran. That makes knowing exactly how they'd go about it more difficult.
"Those will be resilience tests for us," Mark Montgomery, director of the Cyberspace Solarium Commission's succeeding group CSC 2.0, said of the range of potential cyberstrikes from China.
Here are what a few of the most likely scenarios could look like.

Military and transportation networks
Military systems and transportation methods for troops and supplies to come to Taiwan's aid are likely to be at the top of the list for Chinese hackers.

President Joe Biden has committed multiple times to sending U.S. troops to Taiwan in the event of a Chinese invasion, something China would want to stop. This could include targeting the networks of ports on the West Coast, airfields, and other transportation networks that move troops.

"If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide," the U.S. intelligence community's annual threats assessment, released in February, warned.

The report stressed that "such a strike would be designed to deter U.S. military action by impeding U.S. decision making, inducing societal panic and interfering with the deployment of U.S. forces."

Interrupting operations at ports would be a top priority. Gallagher and Rep. Carlos Giménez (R-Fla.) recently visited the Port of Miami to highlight Chinese investment in U.S. ports infrastructure. This included noting that the vast majority of cargo cranes at ports come from one Chinese company.

The lawmakers alleged that China could shut down the cranes to delay aid to Taiwan. Republican leaders of the House Homeland Security Committee subsequently sent a letter to DHS asking about cyber vulnerabilities at maritime ports.
"If an adversary exploits the operational technology (OT) system of these cranes, port operations could completely shut down," the lawmakers wrote.

When House Republicans ran through a Chinese invasion of Taiwan scenario at their policy retreat in Florida last month, cybersecurity quickly came up as an issue.

One member, playing the role of the secretary of Homeland Security, was forced to pick between three options on how to best use limited U.S. cyber defense resources: Defend networks critical to military deployment, focus on protecting networks used for day-to-day life or fight a widespread Chinese disinformation campaign online. The member chose the military networks.

Montgomery, who helped run the program, said the scenario made clear that while the member's decision to defend military networks helped the U.S. win the fight, "we have insufficient cyber and physical critical infrastructure protection capacity in the United States."

Energy

Chinese hackers also would be likely to zero in on U.S. critical infrastructure in order to undermine Americans' support for Taiwan.

This could include going after electricity operators and fuel suppliers. A 2021 ransomware attack on a major East Coast gasoline supplier temporarily caused widespread gas shortages and led to long lines at the pump, illustrating the societal disruption that a cyberattack can cause.

Cybersecurity and Infrastructure Security Agency Director Jen Easterly predicted in February that Chinese hackers could go after systems like gas pipelines, warning that this type of attack would try to divide Americans. Easterly, whose agency is charged with protecting U.S. critical infrastructure against cyber threats, said China would use cyberattacks against the U.S. to sow "panic and chaos."

"I think they, in the event that they go after Taiwan, are going to want to make sure they affect the unity that has been forged between the U.S. and our international partners, the unity that has been forged within the U.S.," Easterly said of Chinese hacking threats.

Water

The water sector, widely viewed as one of the most vulnerable areas for attack, could also come under threat from China. The potentially disastrous effects of a cyberattack on this sector were demonstrated in 2021, when an unidentified hacker gained access to networks at a water treatment center in Oldsmar, Fla., and tried — but failed — to poison the water supply.

The Biden administration has begun to address security vulnerabilities in the sector, but it may not be enough to counter threats from China, which has shown interest in hacking the water sector in recent years. This has included alleged targeting of a water district in Southern California, the nation's largest water agency, through a widely-used vulnerability.

Making things worse is how under-resourced many water sector organizations are, with many smaller groups having neither the funding or personnel to respond to cyber threats. This is making the crucial sector a sitting duck for attacks.

Businesses and Financial Markets
In China's history of hacking U.S. companies, it has often prioritized financial gain and stealing intellectual property. China will likely continue to pursue these goals in an invasion of Taiwan, and try to hit U.S. financial markets, both in a bid to undermine U.S. support for Taiwan, and to cause chaos.

In the scenario run through by House Republicans last month, the finance sector was the main casualty of focusing cyber war-fighting capabilities on military mobilization instead of protecting civilian networks.
"A side effect will be that it impacts the resilience of your financial services," Montgomery said.

Hits to the financial sector, along with any companies critical to getting troops mobilized, could also play into China's bid to slow down military operations.
"The Department of Defense, for military mobilization purposes, relies on the national critical infrastructure, power, water, transportation, even financial services, so to the degree that the national critical infrastructure is not ready, the military will be hampered," Montgomery said.

Preparations on the home front
Should China pursue any of these avenues for crippling the U.S., it may not have an easy fight.

While experts warn that the U.S. has more vulnerabilities than most nations due to the highly interconnected and online nature of most organizations, this does not mean that the U.S. is defenseless.

The U.S. is seen as one of the most advanced nations in cyberspace, though specifics of these abilities are closely guarded intelligence secrets. The U.S. military blocked the internet access of Russia's top troll farm on the day of the 2018 midterm elections to stop the spread of disinformation.

And more than a decade ago, U.S. and Israeli intelligence likely carried out a joint cyberattack on an Iranian nuclear enrichment site that set the Iranian nuclear program back.

"China has to worry about our capabilities, and they have to put it as part of their equation," Senate Foreign Relations Chair Bob Menendez (D-N.J.) said. "Every action has a reaction."

Congress has its eyes firmly on China this year, in particular Chinese cyber threats. Gallagher told reporters in February that the new House Select Committee on China will make identifying Chinese cyber threats linked to an invasion of Taiwan a high priority.

He said that the House Armed Services Committee's Subcommittee on Cyber, Innovative Technologies and Information Systems, which he chairs, will also look into this.

“Part of CITI's role,” Gallagher said, “is to ensure the Department of Defense and the private sector are moving with a sense of urgency to harden this critical infrastructure before it's too late.”