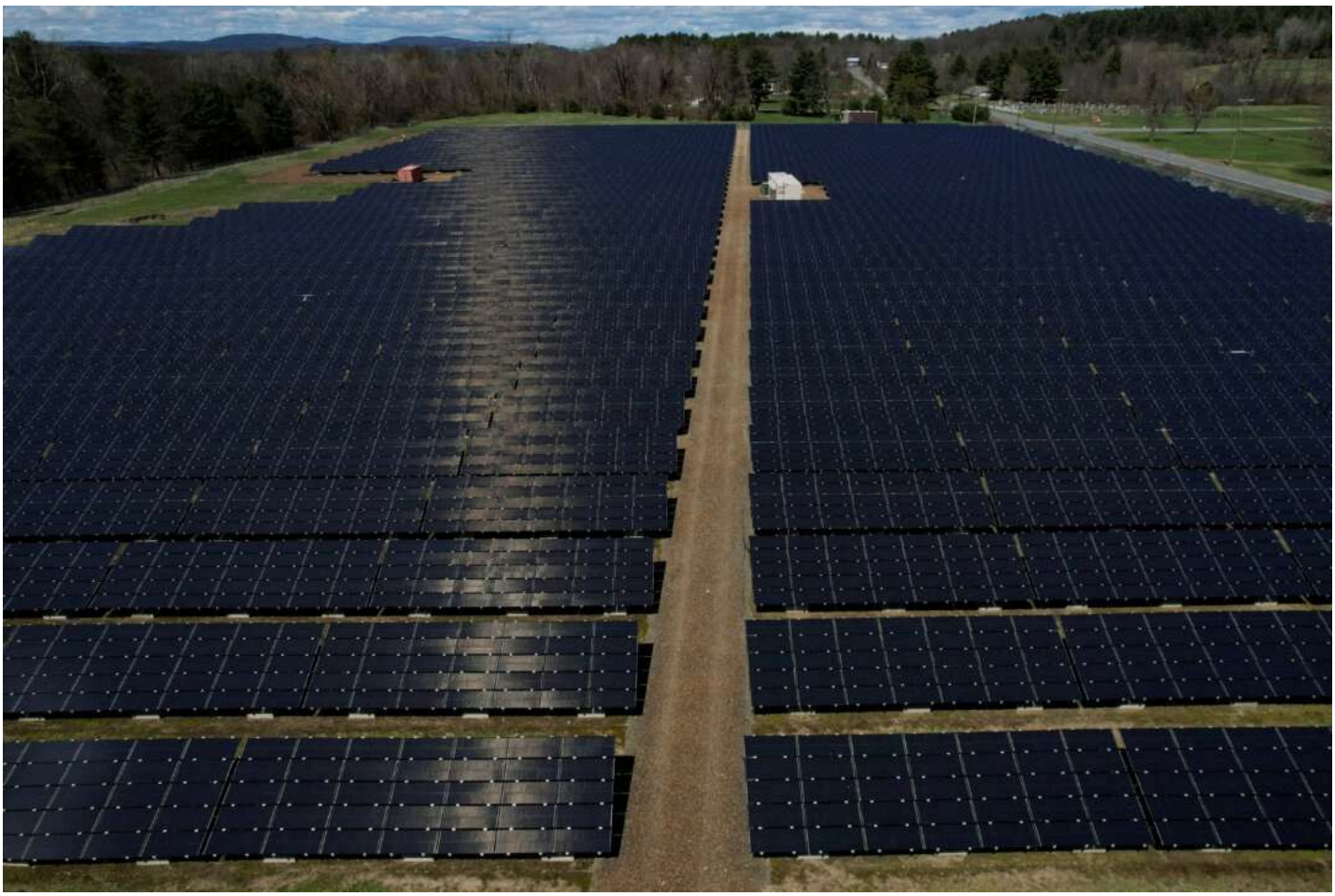
Rogue Communication Devices Found in Chinese Solar Power Inverters

The rogue components provide additional, undocumented communication channels that could allow firewalls to be circumvented remotely.



Solar panels are arrayed on Earth Day in Northfield, Mass., on April 22, 2022. Brian Snyder/Reuters

REUTERS

By Reuters

5/15/2025 Updated: 5/15/2025

LONDON—U.S. energy officials are reassessing the risk posed by Chinese-made devices that play a critical role in renewable energy

infrastructure after unexplained communication equipment was found inside some of them, two people familiar with the matter said.

Power inverters, which are predominantly produced in China, are used throughout the world to connect solar panels and wind turbines to electricity grids. They are also found in batteries, heat pumps, and electric vehicle chargers.

While inverters are built to allow remote access for updates and maintenance, the utility companies that use them typically install firewalls to prevent direct communication back to China.

However, rogue communication devices not listed in product documents have been found in some Chinese solar power inverters by U.S experts who strip down equipment hooked up to grids to check for security issues, the two people said.

Over the past nine months, undocumented communication devices, including cellular radios, have also been found in some batteries from multiple Chinese suppliers, one of them said.

Reuters was unable to determine how many solar power inverters and batteries they have looked at.

The rogue components provide additional, undocumented communication channels that could allow firewalls to be circumvented remotely, with potentially catastrophic consequences, the two people said.

Both declined to be named because they did not have permission to speak to the media.

“We know that China believes there is value in placing at least some elements of our core infrastructure at risk of destruction or disruption,” said Mike Rogers, a former director of the U.S. National Security Agency. “I think that the Chinese are, in part, hoping that the widespread use of inverters limits the options that the West has to deal with the security issue.”

Using the rogue communication devices to skirt firewalls and switch off inverters remotely, or change their settings, could destabilize power grids, damage energy infrastructure, and trigger widespread blackouts, experts said.

“That effectively means there is a built-in way to physically destroy the grid,” one of the people said.

The two people declined to name the Chinese manufacturers of the inverters and batteries with extra communication devices, nor say how many they had found in total.

The existence of the rogue devices has not previously been reported. The U.S. government has not publicly acknowledged the discoveries.

Asked for comment, the U.S. Department of Energy (DOE) said it continually assesses risk associated with emerging technologies and that there were significant challenges with manufacturers disclosing and documenting functionalities.

“While this functionality may not have malicious intent, it is critical for those procuring to have a full understanding of the capabilities of the products received,” a spokesperson said.

Work is ongoing to address any gaps in disclosures through the implementation of “software bills of materials”—or inventories of all the components that make up a software application—and other contractual requirements, the spokesperson said.

Trusted Equipment

As U.S.–China tensions escalate, the United States and others are reassessing China’s role in strategic infrastructure because of concerns about potential security vulnerabilities, two former government officials said.

“The threat we face from the Chinese Communist Party (CCP) is real and growing. Whether it’s telecom hacks or remotely accessing solar and battery inverters, the CCP stops at nothing to target our sensitive infrastructure and components,” said Rep. August Pfluger (R-Texas), a member of the Committee on Homeland Security.

“It is about time we ramp up our efforts to show China that compromising us will no longer be acceptable.”

In February, two U.S. senators introduced the Decoupling From Foreign Adversarial Battery Dependence Act, banning the Department of Homeland Security from purchasing batteries from some Chinese entities, starting October 2027, due to national security concerns.

The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs on March 11 and has yet to be enacted.

It aims to prevent Homeland Security from procuring batteries from six Chinese companies Washington says are closely linked to the CCP:

Contemporary Amperex Technology Co. (CATL), BYD Co., Envision Energy, EVE Energy Co., Hithium Energy Storage Technology Co., and Gotion High-Tech Co.

None of the companies responded to requests for comment.

Utilities are now preparing for similar bans on Chinese inverter manufacturers, three people with knowledge of the matter said.

Some utilities, including Florida's largest power supplier Florida Power & Light Co., are attempting to minimize the use of Chinese inverters by sourcing equipment from elsewhere, according to two people familiar with the matter. FPL did not respond to requests for comment.

The DOE spokesperson said, "As more domestic manufacturing takes hold, DOE is working across the federal government to strengthen U.S. supply chains, providing additional opportunities to integrate trusted equipment into the power grid."

'Catastrophic Implications'

Huawei is the world's largest supplier of inverters, accounting for 29 percent of shipments globally in 2022, followed by Chinese peers Sungrow and Ginlong Solis, according to consultancy Wood Mackenzie.

German solar developer 1Komma5 said, however, that it avoids Huawei inverters, because of the brand's associations with security risks.

"Ten years ago, if you switched off the Chinese inverters, it would not have caused a dramatic thing to happen to European grids, but now the critical mass is much larger," 1Komma5 Chief Executive Philipp Schroeder said.

"China's dominance is becoming a bigger issue because of the growing renewables capacity on Western grids and the increased likelihood of a prolonged and serious confrontation between China and the West."

Since 2019, the United States has restricted Huawei's access to U.S. technology, accusing the company of activities contrary to national security, which Huawei denies.

Chinese companies are required by law to cooperate with China's intelligence agencies, giving the government potential control over Chinese-made inverters connected to foreign grids, experts said.

While Huawei decided to leave the U.S. inverter market in 2019—the year its 5G telecoms equipment was banned—it remains a dominant supplier elsewhere.

Huawei declined to comment.

In Europe, exercising control over just three to four gigawatts of energy could cause widespread disruption to electricity supplies, experts said.

The European Solar Manufacturing Council estimates over 200 GW of European solar power capacity is linked to inverters made in China—equivalent to more than 200 nuclear power plants.

At the end of last year, there was 338 GW of installed solar power in Europe, according to industry association SolarPower Europe.

“If you remotely control a large enough number of home solar inverters, and do something nefarious at once, that could have catastrophic implications to the grid for a prolonged period of time,” said Uri Sadot, cyber security program director at Israeli inverter manufacturer SolarEdge.

Strategic Dependencies

Other countries such as Lithuania and Estonia acknowledge the threats to energy security. In November, the Lithuanian government passed a law blocking remote Chinese access to solar, wind, and battery installations above 100 kilowatts—by default restricting the use of Chinese inverters.

Lithuanian Energy Minister Zygimantas Vaiciunas said this could be extended to smaller rooftop solar installations.

Estonia’s director general of the Foreign Intelligence Service, Kaupo Rosin, said the country could be at risk of blackmail from China if it did not ban Chinese technology in crucial parts of the economy, such as solar inverters.

Estonia’s Ministries of Defense and Climate declined to comment when asked if they had taken any action.

In Britain, the government’s review of Chinese renewable energy technology in the energy system—due to be concluded in the coming months—includes looking at inverters, a person familiar with the matter said.

In November, solar power inverters in the United States and elsewhere were disabled from China, highlighting the risk of foreign influence over local electricity supplies and causing concern among government officials, three people familiar with the matter said.

Reuters was unable to determine how many inverters were switched off, or the extent of disruption to grids. The DOE declined to comment on the incident.

The incident led to a commercial dispute between inverter suppliers Sol-Ark and Deye, the people said.

“Sol-Ark does not comment on vendor relationships, including any relationship with Deye, nor does it have any control over inverters that are not branded Sol-Ark, as was the case in the November 2024 situation you referenced,” a Sol-Ark spokesperson said.

Deye did not respond to requests for comment.

The energy sector is trailing other industries such as telecoms and semiconductors, where regulations have been introduced in Europe and the United States to mitigate China’s dominance.

Security analysts say this is partly because decisions about whether to secure energy infrastructure are mostly dictated by the size of any installation.

Household solar or battery storage systems fall below thresholds where security requirements typically kick-in, they said, despite now contributing a significant share of power on many Western grids.

NATO, the 32-country Western security alliance, said China’s efforts to control member states’ critical infrastructure—including inverters—were intensifying.

“We must identify strategic dependencies and take steps to reduce them,” a NATO official said.

By Sarah McFarlane

Reuters
Author

Author's Selected Articles

At Least 21 People Dead in Mexico After Multi-Vehicle Highway Accident

May 15, 2025

Sean 'Diddy' Combs's Ex-girlfriend Says He Raped Her, Paid $20 Million in Settlement

May 14, 2025

Strong Earthquake Strikes Off Crete, No Damage Reported

May 13, 2025

Sean 'Diddy' Combs Trial: Day One Takeaways

May 12, 2025