# Us regulators intensify probes into Chinese solar inverters harbouring secret communications



U.S. energy officials are stepping up their scrutiny of Chinese-manufactured solar power inverters and batteries following alarming discoveries of rogue communication devices integrated within these units. These inverters, which are essential for linking renewable energy sources like solar panels and wind turbines to electricity grids, have been found to contain undocumented communication equipment that could undermine established security protocols. The presence of these unapproved devices raises significant concerns over potential remote manipulation of critical energy infrastructure, raising fears of widespread blackouts and destabilisation of power grids.

These power inverters, predominantly produced in China, are designed to allow remote access for maintenance and updates. However, utility companies typically employ firewalls to protect against direct communications from Chinese manufacturers. Recently, experts have uncovered cellular radios and other communication devices concealed within some of these inverters. Over the past nine months, they have also detected similar undocumented components in batteries supplied by various Chinese manufacturers. The implications of such findings are grave; analysts warn that circumvention of firewalls could allow attackers to alter settings or disable inverters, posing a substantial risk to energy infrastructure.

Mike Rogers, former director of the U.S. National Security Agency, articulated the broader security risks, stating, “We know that China believes there is value in placing at least some elements of our core infrastructure at risk of destruction or disruption.” The response from congressional leaders has been swift. U.S. Representative August Pfluger expressed an urgent need to confront these threats, asserting that the actions of the Chinese Communist Party represent a tangible danger to Western infrastructures.

This escalation in scrutiny coincides with rising tensions between the U.S. and China. New legislative measures have been proposed, such as the Decoupling from Foreign Adversarial Battery Dependence Act, which seeks to prohibit the Department of Homeland Security from sourcing batteries from certain Chinese companies due to national security concerns. The affected companies include industry giants like Contemporary Amperex Technology Company and BYD. With these developments, utilities across the country are actively seeking to reduce their dependency on Chinese inverters by exploring alternative sources.

Notably, as concerns mount over the global dominance of Chinese inverter manufacturers—Huawei alone accounted for 29% of global shipments in 2022—industries in other parts of the world are also grappling with similar challenges. In the European context, the growing reliance on Chinese technology has stirred fears of vulnerability. The European Solar Manufacturing Council estimates that over 200 gigawatts of solar capacity in Europe is linked to Chinese-made inverters, a connection that could translate into significant risks if foreign influence were to extend into national energy grids.

Several nations have already taken steps to mitigate these threats. For example, Lithuania has recently enacted legislation to restrict remote access by Chinese manufacturers to solar and wind power plants. This move reflects a growing recognition of the critical need for greater cybersecurity measures in energy infrastructure, a sentiment echoed by analysts and governmental officials across Europe and North America.

The risks posed by undocumented communication devices are not merely theoretical. Cybersecurity incidents involving solar power systems have already been documented, with evidence suggesting potential backdoor access to installations enabling hackers to alter operational parameters or access sensitive user data. The North American Electric Reliability Corporation has warned that deficiencies in inverter technology could disrupt bulk power supplies, raising alarms about the overall stability of the grid.

The energy sector, now under scrutiny for its reliance on foreign technology, needs to implement stringent regulatory frameworks akin to those already established for telecommunications and semiconductors. As cybersecurity vulnerabilities become increasingly apparent, the drive for energy independence and a secure, reliable infrastructure has never been more essential.

Ultimately, the ongoing tension surrounding Chinese-made energy technology highlights a broader narrative of strategic dependencies and the imperative to fortify vital infrastructure against potential cyber threats. As nations confront the reality of an interconnected world, the need for vigilance and proactive measures to safeguard energy security becomes critical.

### Reference Map

1. Paragraphs 1-2: [[1]](https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)
2. Paragraphs 3-4: [[1]](https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/), [[3]](https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html)
3. Paragraph 5: [[1]](https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/), [[6]](https://www.jdsupra.com/legalnews/cybersecurity-and-solar-power-7710406/)
4. Paragraphs 6-7: [[1]](https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/), [[4]](https://www.pv-tech.org/lithuania-to-block-chinese-inverters-with-cybersecurity-legislation/)
5. Paragraphs 8-9: [[1]](https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/), [[5]](https://www.pv-magazine.com/2022/09/06/dutch-agency-investigates-cybersecurity-of-pv-inverters-after-hack/)
6. Paragraphs 10-11: [[1]](https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/), [[4]](https://www.pv-tech.org/lithuania-to-block-chinese-inverters-with-cybersecurity-legislation/), [[6]](https://www.jdsupra.com/legalnews/cybersecurity-and-solar-power-7710406/)
7. Paragraphs 12-13: [[1]](https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/), [[3]](https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html)
8. Paragraphs 14-15: [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/), [[6]](https://www.jdsupra.com/legalnews/cybersecurity-and-solar-power-7710406/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.staradvertiser.com/2025/05/15/breaking-news/rogue-devices-found-in-chinese-solar-inverters-raising-u-s-grid-fears/> - Please view link - unable to able to access data
2. <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/> - U.S. energy officials are investigating security threats posed by Chinese-manufactured solar power inverters and batteries after discovering rogue, undocumented communication devices in some units. These inverters are crucial for integrating solar panels, wind turbines, and batteries into electricity grids. Experts fear these components could bypass firewalls, allowing remote manipulation, potentially destabilizing power grids and causing large-scale blackouts. While the Chinese embassy denies malicious intent, U.S. lawmakers and analysts warn of the growing risk of cyber threats from China, especially as Chinese companies dominate the global inverter market.
3. <https://www.csoonline.com/article/2119281/hijack-of-monitoring-devices-highlights-cyber-threat-to-solar-power-infrastructure.html> - An attack on remote monitoring devices in Japan underscores an emerging cybersecurity threat to the rapidly growing solar component of the power grid. Inverters used with solar panels could pose a more significant risk. The North American Electric Reliability Corporation (NERC) has warned that deficiencies in inverters pose a significant risk to bulk power supply reliability and could potentially cause widespread outages. The U.S. Department of Energy warned in 2022 that a cyberattack on inverters could reduce the grid’s reliability and stability.
4. <https://www.pv-tech.org/lithuania-to-block-chinese-inverters-with-cybersecurity-legislation/> - Lithuanian lawmakers have adopted legislation designed to limit the ability of Chinese inverter manufacturers to remotely access the country’s solar and wind power plants. The law imposes greater security measures on electricity generation and information management systems to insulate them from the influence of 'hostile countries,' as designated by the country’s National Security Strategy. From 1 May 2025, operators of new Lithuanian power plants over 100kW in capacity will have to ensure that additional safeguards are in place for the information management systems and inverters at their sites.
5. <https://www.pv-magazine.com/2022/09/06/dutch-agency-investigates-cybersecurity-of-pv-inverters-after-hack/> - The state-run Dutch Radiocommunications Agency has launched an investigation into whether PV inverters pose a threat to the cybersecurity of the electricity system in the Netherlands. A Dutch hacker gained access to PV systems operated via a monitoring tool developed by China’s Solarman. The hacker was able to view the personal data of Dutch customers, create new customers, delete existing users, and download, adjust, and upload inverter firmware. The Solarman spokesperson stated that the problem has been resolved, without any real impact on the affected PV systems.
6. <https://www.jdsupra.com/legalnews/cybersecurity-and-solar-power-7710406/> - Although solar systems historically presented relatively minor risk of cyberattack, the growth in the number of installations and the modernization of solar power components to communicate wirelessly and/or over the Internet have increased risk for these systems. Cyberattacks on solar facilities could cause financial damage by changing where power is delivered, and/or physical damage by hacking inverters to change the voltage or current injected into homes or the grid. The Department of Energy (DOE) advocates multiple layers of protection for solar generation, including anti-virus software in distributed energy resource systems like solar inverters and battery controllers.
7. <https://engineering.uci.edu/news/2020/8/uci-cyber-physical-security-researchers-highlight-vulnerability-solar-inverters> - Cyber-physical systems security researchers at the University of California, Irvine can disrupt the functioning of a power grid using about $50 worth of equipment tucked inside a disposable coffee cup. In a presentation delivered at the Usenix Security 2020 conference, Mohammad Al Faruque and his team revealed that the spoofing mechanism can generate a 32 percent change in output voltage, a 200 percent increase in low-frequency harmonics power, and a 250 percent boost in real power from a solar inverter. The researchers highlighted the vulnerability of solar inverters to cyber-physical attacks.