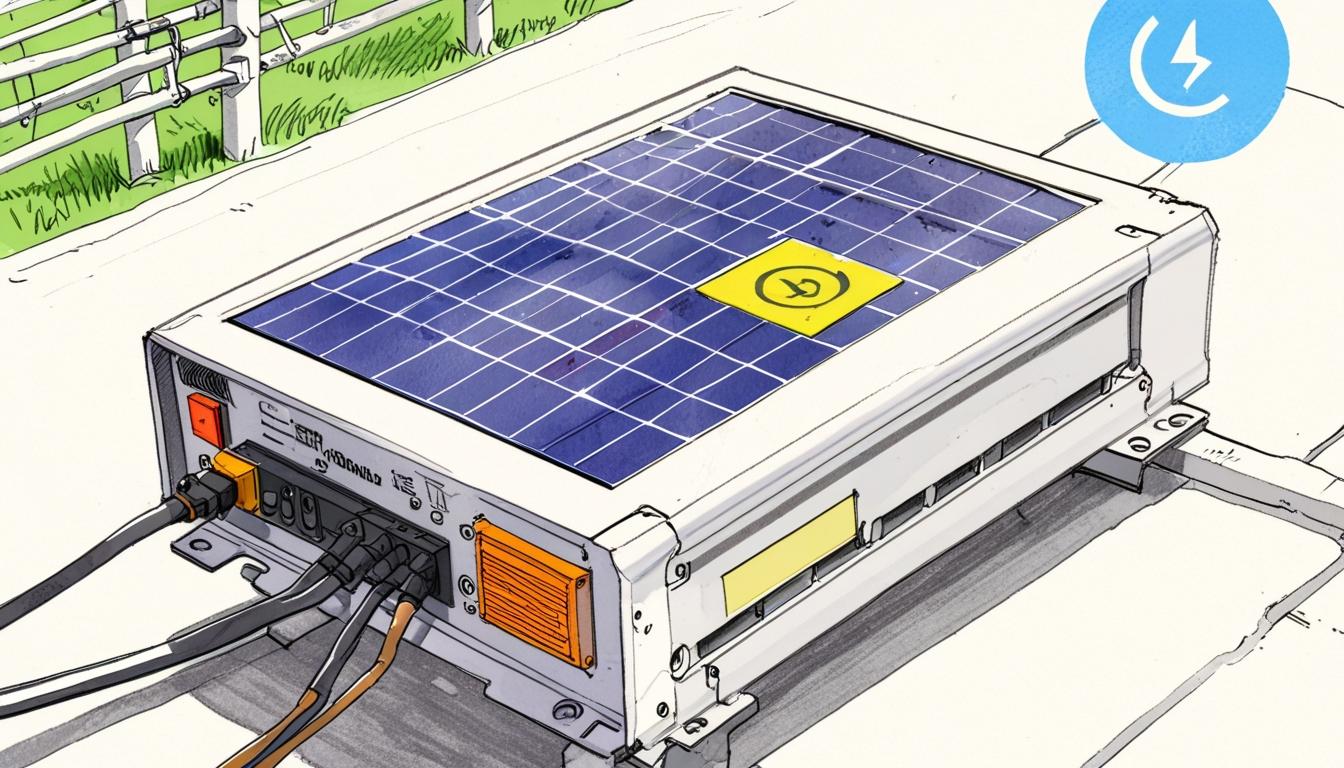
# U.S. probes hidden wireless tech in Chinese solar inverters amid national security fears



U.S. energy officials are currently reassessing the potential security risks posed by Chinese-manufactured power devices, particularly solar inverters. Recent investigations have uncovered undisclosed communication technology embedded within these devices, prompting alarms about the implications for critical infrastructure. Power inverters, essential for linking renewable energy sources such as solar panels and wind turbines to electrical grids, are predominantly produced in China, with major manufacturers including Huawei, Sungrow, and Ginlong Solis.

Recent findings indicate that these inverters may harbour undocumented communication devices, including cellular radios, which could create vulnerabilities by allowing access to energy infrastructure that bypasses established firewalls. As these devices can connect directly back to manufacturers or third parties, the risks associated are substantial. Experts warn that if these rogue channels are exploited, it could result in destabilisation of power grids, damage to energy assets, or even widespread blackouts. This concern is accentuated by the belief that China could leverage such vulnerabilities to exert influence or disrupt services in adversarial nations.

Mike Rogers, a former director of the U.S. National Security Agency, articulated the gravity of the situation, asserting that such devices represent a direct threat to national security. He remarked on the strategic value for China in embedding elements that could potentially disrupt Western infrastructures, pointing to the increasing reliance on these devices amid rising tensions between the U.S. and China.

In response to these revelations, some U.S. utilities are taking proactive measures. For instance, Florida Power & Light Company is exploring alternatives to Chinese inverters to mitigate associated risks. U.S. Senators have also introduced legislation, such as the Decoupling from Foreign Adversarial Battery Dependence Act, which seeks to restrict the Department of Homeland Security from sourcing batteries from specific Chinese companies deemed closely aligned with governmental controls and potentially hostile actions. While this bill has yet to be enacted, it signals a growing concern over foreign technology in essential infrastructure.

The situation is not unique to the U.S. Countries like Lithuania and Estonia have already recognised the cybersecurity threats posed by Chinese technology in energy sectors. Lithuania has enacted legislation to block remote access to major energy installations by Chinese entities, illustrating the seriousness with which these nations are approaching the issue. Estonia’s intelligence reports echo these sentiments, cautioning against reliance on foreign technology that could lead to blackmail scenarios.

Moreover, the repercussions of these security vulnerabilities are magnified by the extensive foothold that Chinese companies have in global markets. As the largest supplier of solar inverters, Huawei accounted for approximately 29% of shipments in 2022 alone. Experts note that the concentration of Chinese manufacture poses a potential risk, especially as Western countries increasingly integrate renewable energy into their power grids.

Concerns extend beyond physical hardware, with security analysts highlighting that internet-connected inverters are increasingly at risk of hacking. This vulnerability could lead to incorrect data measurements, further threatening grid stability. Historical data also suggests an urgent need for more stringent security measures in the energy sector, similar to those already enacted in telecoms and semiconductors, to counteract China's dominant presence.

The intersection of energy security and international relations is complex and evolving. As nations grapple with the critical needs of renewable energy infrastructure alongside national security, the push for transparency and robust cybersecurity measures appears vital. With the revelation of these rogue communication devices, the stakes in managing energy security are higher than ever, underscoring the urgency for nations to reassess their strategies in light of growing geopolitical tensions.

The paradigm shift in energy reliance necessitates vigilance to avoid catastrophic implications for critical infrastructure, highlighting the necessity for continued scrutiny and strategic planning in an increasingly interconnected and technology-driven world.

## Reference Map

* Paragraph 1: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)
* Paragraph 2: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)
* Paragraph 3: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)
* Paragraph 4: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)
* Paragraph 5: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)
* Paragraph 6: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/)
* Paragraph 7: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/), [[6]](https://zenteq.ph/solar-inverters-pose-a-cybersecurity-risk/)
* Paragraph 8: [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/), [[6]](https://zenteq.ph/solar-inverters-pose-a-cybersecurity-risk/)
* Paragraph 9: [[3]](https://www.securityweek.com/many-potential-backdoors-found-huawei-equipment-study/), [[6]](https://zenteq.ph/solar-inverters-pose-a-cybersecurity-risk/)
* Paragraph 10: [[4]](https://www.pv-magazine.com/2024/11/04/grid-resilient-inverters-are-exposed-to-cyber-physical-threats/), [[5]](https://arxiv.org/abs/2409.17873)
* Paragraph 11: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[6]](https://zenteq.ph/solar-inverters-pose-a-cybersecurity-risk/)
* Paragraph 12: [[1]](https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters), [[2]](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/), [[5]](https://arxiv.org/abs/2409.17873)

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

## Bibliography

* <https://www.straitstimes.com/asia/ghost-in-the-machine-rogue-communication-devices-found-in-chinese-inverters> - Please view link - unable to able to access data
* <https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/> - U.S. energy officials are reassessing the security risks of Chinese-made power inverters and batteries after undisclosed communication devices were found in several units. These rogue components, such as cellular radios, create backdoor communication channels that bypass firewalls and potentially allow remote control of critical infrastructure, posing risks like grid destabilization or blackouts. Chinese-produced inverters dominate the global market, with Huawei, Sungrow, and Ginlong Solis leading in shipments. Concerns over China's legal obligation to cooperate with intelligence services amplify fears about foreign control over vital infrastructure. ([reuters.com](https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/?utm_source=openai))
* <https://www.securityweek.com/many-potential-backdoors-found-huawei-equipment-study/> - A report by Finite State reveals that over half of Huawei's enterprise networking products analyzed contained potential backdoors, including default usernames and passwords, hardcoded SSH keys, and numerous known vulnerabilities. The study highlights concerns about Huawei's security posture and the potential risks associated with using their devices. ([securityweek.com](https://www.securityweek.com/many-potential-backdoors-found-huawei-equipment-study/?utm_source=openai))
* <https://www.pv-magazine.com/2024/11/04/grid-resilient-inverters-are-exposed-to-cyber-physical-threats/> - Research indicates that grid-resilient inverters, which provide real-time data and can alert users to faults, are susceptible to cyber-physical threats. These internet-connected devices can be hacked, potentially leading to incorrect measurements and destabilizing the power grid. ([pv-magazine.com](https://www.pv-magazine.com/2024/11/04/grid-resilient-inverters-are-exposed-to-cyber-physical-threats/?utm_source=openai))
* <https://arxiv.org/abs/2409.17873> - A study titled 'ReThink: Reveal the Threat of Electromagnetic Interference on Power Inverters' analyzes the security of photovoltaic inverters, discovering vulnerabilities to electromagnetic interference (EMI) at frequencies of 1 GHz or higher. The research demonstrates that EMI can lead to denial of service, physical damage, or reduced power output in inverters, highlighting the need for enhanced security measures. ([arxiv.org](https://arxiv.org/abs/2409.17873?utm_source=openai))
* <https://zenteq.ph/solar-inverters-pose-a-cybersecurity-risk/> - Concerns have been raised about the cybersecurity risks associated with Chinese-made solar inverters. In the U.S., former Assistant Secretary of Defense Paul Stockton linked these risks to potential attacks on the power grid. Similarly, in Australia, Shadow Minister for Home Affairs and Cyber Security, Senator James Paterson, highlighted vulnerabilities in smart inverters supplied by Chinese manufacturers, including Huawei. ([zenteq.ph](https://zenteq.ph/solar-inverters-pose-a-cybersecurity-risk/?utm_source=openai))
* <https://solar2power.pt/powering-up-risk-inverters-vulnerable-to-cybersecurity-threats-through-software/> - A Dutch hacker infiltrated an inverter connected to Solarman, a solar monitoring software tool owned by a Chinese company. This breach allowed access to sensitive data of Dutch users, including electricity data and GPS coordinates, and manipulation of the client list. The incident underscores the need for robust security and auditing of software portals associated with inverters. ([solar2power.pt](https://solar2power.pt/powering-up-risk-inverters-vulnerable-to-cybersecurity-threats-through-software/?utm_source=openai))