# Concerns rise over kill switches in Chinese-made solar inverters threatening global clean energy security



Concerns are mounting over the security of solar power systems, especially regarding Chinese-manufactured inverters, which play a central role in the integration of renewable energy sources like solar panels and wind turbines into power grids. Recent reports have unveiled the presence of kill switches in these inverters, prompting fears that security vulnerabilities could significantly hinder global efforts to transition to clean energy and meet climate goals.

Investigations by U.S. energy officials have revealed the existence of undocumented communication devices within these inverters, potentially posing severe cybersecurity threats. Experts warn that such devices could bypass existing firewalls, enabling remote manipulation that might destabilise power grids, leading to widespread blackouts. The U.S. has become particularly vigilant given that Chinese companies hold a dominant position in the global inverter market. Despite the Chinese embassy's denials of any malicious intent, analysts and lawmakers express growing concern about the risk of cyber threats emanating from China.

In response to these security challenges, several nations are taking proactive measures. In Lithuania, for instance, lawmakers have enacted legislation to mitigate risks associated with Chinese inverter manufacturers. Under new regulations effective from May 1, 2025, operators of power plants exceeding 100 kW capacity must implement enhanced safeguards for their information management systems and inverters. This development is part of a broader initiative across Europe, where the European Solar Manufacturing Council (ESMC) has proposed the creation of an 'Inverter Security Toolbox'. This toolbox would aim to evaluate risks linked to inverter manufacturers and could potentially include bans on high-risk vendors from connecting to local grids, thereby strengthening the cybersecurity posture of critical energy infrastructure.

Moreover, the concerns are not confined to Europe. In Taiwan, an information security expert has highlighted similar risks posed by inverters produced by Chinese firms, notably Huawei Technologies. With a substantial portion of Taiwan's solar energy systems reliant on such technology, the expert warns of the potential for coordinated shutdowns that could threaten national security. They recommend the establishment of a blacklist to inform consumers about which products to avoid, reflecting a cautious approach towards technology sourced from potentially hostile nations.

The cybersecurity risks associated with solar power systems have been on the rise as installations grow and components become increasingly interconnected. Research shows that modern smart photovoltaic (PV) inverters, controlled through sophisticated SCADA systems, are particularly vulnerable to various cyber intrusions. These vulnerabilities can result in loss of control over energy systems, with intruders gaining access to the entire setup and risking physical damage to the infrastructure.

In light of these challenges, the U.S. Department of Energy advocates for implementing robust security measures, including antivirus software and layered security protocols, to protect distributed energy resource systems like solar inverters. As the global energy landscape continues to evolve towards renewable sources, the need for secure, reliable technology has never been more critical. The combined efforts of governments and industry leaders will determine whether the boom in solar power, which is essential for achieving climate objectives, can proceed without compromising the integrity of vital energy infrastructures.

Ensuring the security of these systems not only mitigates the risks posed by foreign technology but also fosters confidence in the renewable energy transition as nations move towards sustainable futures. The growing recognition of these cybersecurity threats underscores the need for continued vigilance and collaboration among countries to safeguard their energy infrastructures against emerging vulnerabilities.

### Reference Map

1. Paragraphs 1, 2
2. Paragraphs 2, 4
3. Paragraph 3
4. Paragraph 4
5. Paragraph 3
6. Paragraph 6
7. Paragraph 7

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

## Bibliography

1. <https://carbon-pulse.com/398391/> - 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.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. Starting May 1, 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.
4. <https://www.pveurope.eu/inverter/call-eu-inverter-security-toolbox> - The European Solar Manufacturing Council (ESMC) has called for the development of an EU 'Inverter Security Toolbox' to address cybersecurity risks associated with Chinese-manufactured inverters. The ESMC highlights that over 200 GW of European PV capacity is linked to inverters manufactured in China, raising concerns about remote control of a significant portion of Europe's electricity infrastructure. The proposed toolbox would involve a comprehensive risk assessment of inverter manufacturers and may include outright bans for high-risk vendors from connecting to the grid.
5. <https://www.taipeitimes.com/News/taiwan/archives/2023/08/28/2003805394> - An information security expert has raised concerns about the national security risks posed by Chinese-made inverters installed in Taiwan’s solar energy systems. The expert points out that a significant percentage of inverters used in Taiwan are produced by China-based Huawei Technologies Co. These inverters can be remotely controlled, potentially leading to simultaneous shutdowns of solar energy systems, which could pose a serious national security problem. The expert suggests that the government should produce a white list or blacklist of Chinese products to inform the public about which products to avoid.
6. <https://www.mdpi.com/1996-1073/16/16/5904> - This study discusses the cybersecurity issues associated with smart photovoltaic (PV) inverters, which are becoming increasingly vulnerable to various cyber-attacks, including data integrity attacks and communication-based attacks. The research highlights that modern inverters are remotely controlled by SCADA systems communicating through Ethernet or other wireless communications, making them susceptible to cyber intrusions. Such vulnerabilities can lead to loss of control over the converters in the system and provide intruders access to the entire system, potentially causing adverse physical damage to the PV system.
7. <https://www.jdsupra.com/legalnews/cybersecurity-and-solar-power-7710406/> - The article discusses the growing cybersecurity risks associated with solar power systems due to the increasing number of installations and the modernization of solar power components that communicate wirelessly and over the Internet. It highlights incidents where hackers have gained access to solar panels worldwide, leading to potential financial and physical damage. The Department of Energy advocates for multiple layers of protection for solar generation, including antivirus software in distributed energy resource systems like solar inverters and battery controllers, with virus protection and detection on firewalls and servers that integrate those distributed energy resources into aggregate grid operations.