Policy Liaison Group
Sustainable Buildings

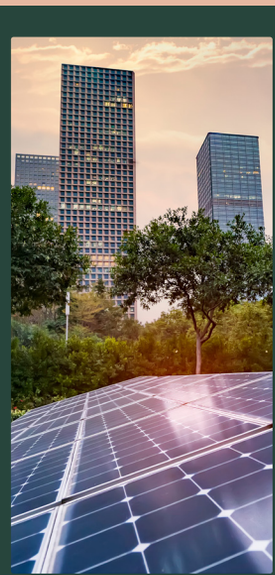
Tuesday 9 September 2025

plgsustainablebuildings.org

Is the UK's solar transition resilient to cyber threats and geopolitical risk?

Christoph Podewils, the European Solar Manufacturing Council (ESMC); Thomas Rührlinger, Fronius; Francis West, Security Everywhere

Westminster



Christoph Podewils

Thomas Rührlinger

Francis West

Introduction

The Policy Liaison Group on Sustainable Buildings convened its inaugural roundtable on energy security, focusing on the risks and opportunities presented by the UK's anticipated solar expansion. With the government's Solar Roadmap targeting a fully decarbonised power system by 2030, solar PV has become central to the UK's clean energy ambitions. However, as participants highlighted, the shift to decentralised, digitalised infrastructure introduces new vulnerabilities in both cybersecurity and supply chains. Concerns were raised about the UK's heavy reliance on Chinese-manufactured components, the systemic risks posed by remotely controllable inverters, and the broader geopolitical implications of supply chain concentration.

This discussion also addressed differing perspectives on whether engagement with Chinese suppliers poses a strategic liability or a necessary route to affordable decarbonisation. The debate underscored the urgency of shaping robust policy responses that balance innovation, security, and resilience in the transition to clean energy.

Key takeaways

Dependence on Chinese solar technology

- Over 60% of UK solar PV equipment, including inverters, is sourced from China. “We are replacing one dependency with another”, a reference to the shift from Russian gas dependency to Chinese solar infrastructure.
- China’s dominance is not accidental, but the result of a decades-long state-led strategy, creating a global dependency for critical infrastructure that risks vulnerability.
- As part of its strategy of rapid growth, China sets the price of solar state-subsidised PV modules. Consumers are dependent on a manually deflated price.

Cybersecurity risks of internet-connected inverters

- Inverters function as the ‘brains’ of PV systems, converting direct current (DC) from panels to alternating current (AC) for the grid. Modern inverters are connected to the internet and remotely controllable. “All European countries, including the UK, are handing over the ability to remotely control critical infrastructure – the electricity system – to China”.
- A coordinated manipulation of just three gigawatts of PV capacity could trigger blackouts in the UK or across Europe. The scale of potential sabotage was likened to controlling “more than 200 nuclear power plants” through software vulnerabilities.

Conflicting views on collaboration with China

- Some contributors argued that leading Chinese manufacturers, particularly “tier 1” suppliers, are reliable partners. They “see us as their consumer”. Their priority is selling commercially competitive products.
- In some cases, Chinese manufacturers apply stricter cyber-security practices than European competitors – e.g. by limiting access to their inverters’ Modbus (the communications channel used to control and monitor devices), reducing the risk of unauthorised control.
- Others stressed that under Chinese law, companies must cooperate with state authorities, making hardware security inseparable from geopolitical considerations.

Broader cybersecurity threats beyond China

- Threats to UK infrastructure are global, not just from China. Malicious attacks from other states, such as North Korea, Russia, and even domestic threats, pose significant risks. Cyberattacks on major UK companies from non-state actors such as Marks & Spencer, Jaguar Land Rover, or the Co-op make clear that threats are not just geostrategic.
- A “house security” analogy was used: many organisations secure the front door, but ignore the “windows and vents”, leaving multiple entry points open to exploitation.

Issues raised

Lack of a clear policy framework

While the EU's Cyber Resilience Act is moving forward, the UK risks lagging behind. Even the hardware supply chain is affected. "It is not possible to buy prefab inverter boards from China without a communication device." Prefab boards are pre-assembled circuit boards that manufacturers integrate into inverters. These components are imported from China with built-in communication modules, wanted or not, meaning every unit is effectively internet-enabled. This raises serious enforcement questions: if policymakers set security standards, but the only available imported hardware already embeds remote-control functions, how can compliance be guaranteed?

Tensions between local authorities and national security

Local councils want to deploy solar and storage at scale – e.g. thousands of social homes. However, local councillors cannot be expected to have the necessary expertise to make informed decisions on PV systems and their potential vulnerabilities. They will want assurances from qualified experts ahead of installation.

Geopolitical context and escalating risks

"Were China to try to take back Taiwan, assets like inverters could be weaponised. It makes perfect strategic sense." China's ownership of supply chain assets, such as in Africa, presents a grey area between dominance over international supply chains and state strategic interests, which can leave consumers threatened by distant geopolitical events.

The urgency of accountability and skills

There's a severe shortage of skilled cyber professionals. Only a third of advertised roles are filled. "The biggest risk to any business is their IT department – giving a false sense of security when it's not their specialism". Without clear frameworks for corporate responsibility, companies cannot be expected to build resilience on their own, making stronger accountability structures and closing the skills gap essential to the UK's cybersecurity.

Recommendations

- **Mandate corporate accountability** – make directors responsible for cyber resilience in energy systems.
- **Embed supply chain transparency** – extend due diligence rules to cover cybersecurity risks.
- **Integrate resilience into strategy** – link cybersecurity directly into energy and industrial plans.
- **Close the cyber skills gap** – expand training and accreditation for specialist roles.

- **Define trusted suppliers** – set standards to certify secure inverter and component manufacturers.
- **Support local authorities** – provide councils with guidance for secure solar and storage rollouts.

Links

Solar Power Europe, 'Solutions for PV Cyber Risks to Grid Stability'

European Parliament, Commissioner Jørgensen

Reuters, 'Rogue communication devices found in Chinese solar power inverters'

OECD, 'Government support in the solar and wind value chains'

We would like to thank the members of our Advisory Board for their contributions and continuing support.

To get involved, please contact
secretariat@plghousing.org