Berlin, Juli 2025

Positionspapier
Die Cybersicherheit der Photovoltaik erfordert sofortige regulatorische Maßnahmen

Die Photovoltaik (PV) spielt eine bedeutende Rolle für die Stromversorgung in Deutschland. Mit einem stetig steigenden Anteil trägt sie bereits heute, aber auch immer stärker in der Zukunft, wesentlich zur Dekarbonisierung des Energiesektors bei. Dies umfasst sowohl gewerbliche PV-Anlagenparks als auch Aufdachanlagen von Privathaushalten – letztere stehen im Fokus dieses Positionspapiers. Die zunehmende Dezentralisierung des Energiesystems erfordert Fernsteuerungsinstrumente und drahtlose Verbindungen, um die Anlagen technisch zu verwalten und die Stromproduktion systemdienlich zu steuern. Da die Anzahl privater Aufdachanlagen kontinuierlich zunimmt und sich zu einer kritischen Menge an Produktionskapazität aggregiert, müssen strenge Cybersicherheitsmaßnahmen ergriffen werden, um die Netzstabilität zu gewährleisten und das gesamte Energiesystem zu schützen.

Um den Risiken politisch angemessen zu begegnen, halten wir folgende Maßnahmen für unerlässlich:

1. Betreiber oder Hersteller von PV-Anlagen, die auf mehr Kapazität als 104 MW zugreifen können und daher als kritische Infrastruktur gelten, sollten nicht unter der direkten oder indirekten Kontrolle von Drittländern und deren Institutionen stehen.
2. Der Zugriff auf die Fernsteuerung von PV-Anlagen über mit dem Internet verbundene Wechselrichter muss innerhalb der EU oder in Staaten mit einem gleichwertigen Sicherheitsniveau verbleiben.
3. Es müssen branchenspezifische Cybersicherheitsvorschriften entwickelt werden, um die sichere Fernsteuerung von PV-Anlagen zu gewährleisten, welche ausschließlich von vertrauenswürdigen Herstellern ausgeführt werden kann.

Hintergrund: Das Risikoprofil von PV-Anlagen

Die Photovoltaik ist auf dem Vormarsch – in Deutschland, Europa und weltweit. Im Jahr 2024 stieg die installierte Leistung der Photovoltaik in Deutschland auf knapp 100 Gigawatt (GW), was der Leistung von 80 bis zu 100 Kernkraftwerken entspricht (BMWE/BNetzA). An sonnenreichen Tagen im Sommer deckt die Stromproduktion aus PV-Anlagen nahezu den vollständigen Strombedarf des Landes – im gesamten Juli 2024 trugen Solaranlagen 28,3 Prozent zur Nettostromerzeugung bei (Fraunhofer ISE). Die deutschen Klimaziele sehen vor, bis 2030 215 GW an Photovoltaik zu installieren, um das übergeordnete Ziel von 80 Prozent an erneuerbarer Stromversorgung zu erreichen (EEG 2023).

Dieser ambitionierte Kurs und der notwendige weitere Ausbau der Photovoltaik bringen neue Herausforderungen mit sich:

1. Die Regulierung zur Gewährleistung der Energiesicherheit und Netzstabilität ist heute auf große, zentralisierte Anlagen ausgelegt. Der unter anderem durch die Photovoltaik vorangetriebene Übergang von der zentralen Stromversorgung zu dezentralen Prosumern, die Strom gleichzeitig produzieren und selbst konsumieren, wird im Sicherheitsrahmen (verankert im EnWG, BSIG und der BSI-KritisV) nicht ausreichend berücksichtigt. Gleichzeitig nehmen Cyberangriffe durch staatlich unterstützte Operationen oder kriminelle Cybergruppen über das Einfallstor unsicherer kritischer Komponenten von nicht vertrauenswürdigen Herstellern zu. Die Bedrohung durch ausländische

Akteure oder systemische Rivalen wurde durch eine Reihe von Cyberangriffen unter anderem auf das US-Unternehmen AMSC (DOJ) und das Bundesamt für Kartographie und Geodäsie (BKG), das Aufgaben im Bereich kritischer Infrastrukturen wahrnimmt (BMI), deutlich. Erst vor kurzem haben US-Energieexperten unbekannte Kommunikationsgeräte in PV-Wechselrichtern chinesischer Hersteller gefunden (Reuters) – die genauen Umstände sind noch ungeklärt. In diesem Zusammenhang ist besonderes Augenmerk auf Regelungen wie das chinesische Spionageabwehrgesetz zu legen, das in China registrierte Unternehmen dazu verpflichtet, die Sicherheitsbemühungen des Staates zu unterstützen.

2. Die Digitalisierung des Energiesystems, die aus Gründen der Effizienz und Flexibilität unerlässlich ist, erfordert einen erhöhten Bedarf an Fernsteuerung und letztlich Vernetzung mit dem Internet. Im Februar 2025 wurden mit dem sogenannten „Solarspitzengesetz“, einer Novelle des Erneuerbare-Energien-Gesetzes (EEG) und weiterer relevanter Energieregulierungen, Digitalisierungsmaßnahmen eingeführt. Dazu zählt die Verpflichtung zur Ausstattung neuer PV-Anlagen mit einer Leistung von mehr als 7 Kilowatt (kW) mit intelligenten Zählern und Steuerungsgeräten (§ 29 (1) MsbG). Viele PV-Bestandsanlagen in Deutschland sind jedoch bereits heute digitalisiert und über den Wechselrichter mit dem Internet verbunden. Der Wechselrichter ist das Herzstück jeder PV-Anlage und zuständig für die Umwandlung des Stroms (Gleichstrom zu Wechselstrom). Die Internetverbindung ermöglicht die Fernsteuerung und Kontrolle der gesamten PV-Anlage durch die Hersteller der Wechselrichter. Bei den meisten PV-Aufdachanlagen ist so ein direkter Zugriff auf die Wechselrichter möglich, ohne dass eine lokale Behörde eingeschaltet werden muss.

Diese Risiken wurden von politischen Akteuren in Deutschland kürzlich erkannt. So hat beispielsweise das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einem am 21. Mai 2025 veröffentlichten Positionspapier die Notwendigkeit einer Erhöhung der Sicherheit für dezentrale Energieanlagen festgestellt. Darin werden Wechselrichter als wichtiger Angriffspunkt identifiziert, der beim Erreichen einer kritischen Anzahl von Anlagen bzw. Kapazität letztlich zu einer Destabilisierung des Stromnetzes führen kann. Entsprechend müssen die Sicherheitsanforderungen auf alle Akteure im Energiesystem, insbesondere die Hersteller kritischer Komponenten, ausgeweitet werden.

Angesichts der stetig wachsenden Bedeutung der Photovoltaik für die Stromversorgung in Deutschland ist es von entscheidender Bedeutung, PV-Anlagen besser vor dem Risiko zu schützen, von Dritten kompromittiert oder als Druckmittel eingesetzt zu werden. Der überwiegende Teil der in Deutschland errichteten PV-Anlagen fällt nicht unter die Definition der kritischen Energieinfrastruktur (Schwellenwert >104 MW) und unterliegt damit keinen strengen Sicherheitsvorgaben. Politik und Regulierungsbehörden müssen daher durch präzise regulatorische Änderungen sicherstellen, dass das Risiko destruktiver Angriffe durch externen Zugriff minimiert wird.

Vorgeschlagene Maßnahmen: Stärkung der Cybersicherheit von PV-Anlagen

Ein gezielter Ausfall von 3 GW Stromerzeugungskapazität kann bereits erhebliche Auswirkungen auf das europäische Stromnetz haben. Dabei ist zu beachten, dass in Europa nur zwei chinesische Unternehmen eine Kapazität von beinahe 200 GW PV über die von ihnen verbauten Wechselrichter kontrollieren (DNV) – dies entspricht etwa der Leistung von 180 Kernkraftwerken. In Deutschland stammen rund 80 Prozent der PV-Wechselrichter auf Privatdächern aus China. Dabei können 70 bis 90 Prozent der an das europäische Stromnetz angeschlossenen Wechselrichter in PV-Anlagen ferngesteuert werden und sind somit potenzielle Ziele für feindliche Manipulationen.

Zum Schutz dezentraler PV-Anlagen sowie zur Stärkung der Netzstabilität und somit der Energiesicherheit Deutschlands schlagen wir folgende Maßnahmen vor, welche im Rahmen des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) umgesetzt werden sollten:

- Erweiterung der rechtlichen Definition des Begriffs „kritische Infrastruktur“ auf Hersteller kritischer Komponenten, wie beispielsweise Wechselrichter, die über Fernzugriff eine aggregierte dezentrale PV-Kapazität von über 104 MW direkt kontrollieren und letztlich die Funktionsfähigkeit der Anlagen

beeinflussen können. Generell ist es wichtig, dass der Gesetzgeber im Rahmen der Regulierung die Sicherheit einzelner (Aufdach-)PV-Anlagen garantiert, die akkumuliert eine hohe Kapazität an Erzeugungsleistung generieren – die ausschließliche Kontrolle von Komponenten der Anlage oder des Systems zur Bündelung elektrischer Leistung und Steuerung von Erzeugungsanlagen oder dezentraler Energieerzeugungsanlagen (BSI-KritisV, Anhang 1) ist nicht ausreichend.

- Nur vertrauenswürdige Hersteller von Komponenten dürfen per Fernsteuerung auf die PV-Anlagen über mit dem Internet verbundene Wechselrichter zugreifen, sofern dieser Zugriff innerhalb der EU oder in Staaten mit einem gleichwertigen Sicherheitsniveau erfolgt. Diese Regelung muss sowohl die direkte Steuerung als auch die indirekte Steuerung über Firmware- und Software-Updates umfassen.
- Die Identifikation und Anzeigepflicht kritischer Komponenten (§9b BSIG) sollte nicht bei dem Betreiber kritischer Energieanlagen, sondern wie in einer vorherigen Entwurfsfassung des NIS2UmsuCG (Entwurf datiert vom 02.12.2024) proaktiv beim Bundesministerium des Inneren (BMI) liegen. Dabei sollte das BSI dann in der Bestimmung der kritischen Komponenten (basierend auf dem Funktionenkatalog der BNetzA in Absprache mit dem BSI) auch die Hersteller (u.a. von Wechselrichtern) im Beratungsprozess konsultieren.

Die Sicherheit der deutschen Stromversorgung und die Stabilität des Stromnetzes ist von essenzieller Bedeutung, bei der keine Kompromisse gemacht werden sollten. Entsprechend fordern wir die politischen Verantwortlichen auf, dieser wichtigen Aufgabe regulatorisch Rechnung zu tragen.

Über SolarEdge

SolarEdge ist ein weltweit führender Anbieter für Smart Energy. Durch erstklassige Ingenieursleistung und Fokus auf Innovation schafft SolarEdge intelligente Lösungen, die unser Leben erleichtern und den Fortschritt vorantreiben. SolarEdge hat eine intelligente Wechselrichterlösung entwickelt, die die Produktion und Verwaltung von Energie in Photovoltaikanlagen grundlegend verändert hat. Der DC-optimierte Wechselrichter von SolarEdge zielt darauf ab, die Stromerzeugung zu maximieren und gleichzeitig die Kosten für die von der PV-Anlage erzeugten Energie zu senken. SolarEdge treibt die Entwicklung von Smart Energy weiter voran und bedient mit seinen Lösungen für PV, Speicher, das Aufladen von Elektroautos und Netzdienstleistungen ein breites Spektrum von Marktsegmenten der Energiebranche. SolarEdge ist online unter der Adresse solaredge.com zu erreichen.

Kontaktpersonen:
Despina Manousos, Head of Government Affairs Europe | [redacted]
Alfred Karlstetter, Senior Advisor | [redacted]