Der Iran legt ein britisches Kraftwerk für vier Tage lahm, aber das ist keine große Sache…

geschrieben von Andreas Demmig | 10. September 2026

Von Jo Nova

Netto-Null macht unsere Stromnetze anfällig

Australier wissen es vielleicht nicht, aber iranische Hacker legten im Juli ein britisches Kraftwerk lahm, und es dauerte vier Tage, bis es wieder in Betrieb genommen werden konnte. Doch es besteht kein Grund zur Sorge. Das britische Kraftwerk war so klein und der Vorfall so unbedeutend, dass die britische Regierung erst nach Wochen davon berichtete und den Namen des Kraftwerks immer noch nicht preisgibt. Es stellte aber absolut keine Bedrohung für das britische Stromnetz dar. Gar keine. Es hätte sich lediglich um einen „Kleingenerator" gehandelt, was bedeutet, dass es sich auch um eine Windkraftanlage gehandelt haben könnte. Zeitungen sprachen jedoch von „Personal", und Clark Savage von *EnergyNewsBeat* bezeichnet es als Spitzenlastkraftwerk. Alles in Ordnung also, oder?

Wenn es der Iran war und er nur ausprobieren wollte, was er tun kann, dann ist das Experiment gelungen.

Der Angriff erfolgte offenbar als Reaktion darauf, dass Großbritannien den USA die Erlaubnis erteilt hatte, Angriffe auf Teheran von britischen Stützpunkten aus durchzuführen. Zeitgleich gab es auch Cyberangriffe auf die USA, bei denen Wasserpumpen manipuliert wurden und dadurch Warnungen vor nicht abgekochtem Trinkwasser ausgelöst wurden. Obwohl keiner dieser Angriffe unmittelbaren Schaden verursachte, zeigt er doch, dass Hackerangriffe bereits Realität sind. Wir wollen wohl kaum ein fragiles Stromnetz, das von Wind und Wolken, langen Übertragungsleitungen und einer Million Wechselrichtern eines anderen Landes abhängig ist, welches dafür bekannt ist, manipulierte Kommunikationsgeräte in seine Solarwechselrichter einzubauen. Ganz zu schweigen von den in Heimbatterien versteckten Sprengsätzen . Australien besitzt dank des Programms zur billigeren Herstellung von Heimbatterien mittlerweile eine halbe Million davon.

Wie wir damals schon sagten, ist es einfach, jedes noch so kleine Teil einer riesigen, zentralisierten Anlage zu überprüfen. Jeder, der die Anlage betritt, kann kontrolliert werden. Es ist jedoch unmöglich, vier Millionen Dachwechselrichter zu inspizieren, die von 500 Unternehmen über acht verschiedene Häfen und aus 20 verschiedenen Fabriken importiert werden. Das dezentrale Netto-Null-System schafft bewusst

Millionen elektronisch gesteuerter Endpunkte, darunter auch Ladestationen für Elektrofahrzeuge, intelligente Zähler, Batteriespeicher für virtuelle Kraftwerke und staatlich gesteuerte Klimaanlagen – viele davon fernsteuerbar und viele letztendlich über Netzwerke miteinander verbunden.

Es geht hier nicht um vier Millionen neue, zufällige Fehlerquellen, sondern vielmehr darum, dass wir 4 Millionen Geräte (vielleicht sogar 10 Millionen) mit einer *systematischen Schwachstelle haben, die ausgenutzt werden kann.*

> # Iranian hackers 'shut down British power plant for four days' in unprecedented cyber attack
>
> - **See more Daily Mail on Google - save us as a Preferred Source**
>
> By FRANCINE WOLFISZ, NEWS REPORTER
> **PUBLISHED:** 01:59 BST, 23 August 2026 | **UPDATED:** 12:15 BST, 23 August 2026
>
> **Iranische Hacker legten britisches Kraftwerk in einem beispiellosen Cyberangriff für vier Tage lahm**
>
> **– Daily Mail UK**
>
> Wie nun bekannt wurde, legten iranische Hacker ein britisches Kraftwerk für vier Tage lahm – ein beispielloser Cyberangriff auf Großbritannien. Die Cyberterroristen zwangen die Anlage zur vollständigen Stilllegung, während die Mitarbeiter fieberhaft daran arbeiteten, die Systeme wieder in Betrieb zu nehmen.
>
> Die Behörden haben nicht bekannt gegeben, welches Kraftwerk das Ziel des Angriffs war, aber es wird davon ausgegangen, dass es relativ klein ist – und der Angriff keine nennenswerten Auswirkungen auf die Energieversorgung des Landes hatte.
>
> Laut Quellen gegenüber CBS News wurden auch Wasserversorgungssysteme in USA, in Dutzenden Bundesstaaten, darunter Michigan, Minnesota, Georgia, New Jersey und South Dakota, von mutmaßlichen Cyberangriffen mit Verbindungen zum Iran getroffen; allein in Minnesota wurden mehr als 30 kommunale Wasserversorgungssysteme angegriffen.

Kathryn Porter verdeutlicht, wie leicht das britische „Netto-Null“-Stromnetz durch einen katastrophalen Angriff lahmgelegt werden könnte. Wie wir letztes Jahr in Spanien und 2016 in Südaustralien gesehen haben, können Stromnetze mit geringer Trägheit innerhalb weniger

Hundertstelsekunden zusammenbrechen, sobald Störungen auftreten. Und nichts verdeutlicht die Bedeutung von Trägheit besser als eine Turbine, die 500 Tonnen wiegt und sich 3.000-mal pro Minute dreht.

Die rotierenden Riesenturbinen der Kohle-, Gas-, Kernkraft- und Wasserkraftanlagen absorbieren die Frequenzschocks in beide Richtungen und verschaffen dem Rest des Stromnetzes wertvolle Sekunden, um entsprechend zu reagieren.

Porter weist darauf hin, dass Batterien nur kurzfristig helfen können und auch nur dann, wenn sie geladen sind, wenn ein Generator ausfällt, oder entladen sind, wenn eine große Last wegfällt. Es wird schwierig sein, sich auf beide Eventualitäten und den Dauerbetrieb vorzubereiten.

The National Grid collapses, Britain goes dark... chaos is unleashed: Nightmare scenario that Britain's Net Zero obsession is pushing us ever closer to, by energy expert KATHRYN PORTER

- **See more Daily Mail on Google - save us as a Preferred Source**

By KATHRYN PORTER
PUBLISHED: 19:42 BST, 23 August 2026 | **UPDATED:** 01:37 BST, 24 August 2026

> **Das nationale Stromnetz bricht zusammen, Großbritannien steht im Dunkeln… Chaos bricht aus: Ein Horrorszenario, dem Großbritanniens Netto-Null-Besessenheit uns immer näherbringt – ein Bericht einer Energieexpertin.**
>
> **– KATHRYN PORTER, Daily Mail**
>
> Stellen Sie sich Folgendes vor: Um 20:37 Uhr heute Abend, wenn ein Teil des nationalen Stromnetzes von einem akuten Ungleichgewicht zwischen Stromangebot und -nachfrage betroffen ist, bricht das gesamte Netz zusammen. Ein Teil reißt den nächsten mit, wie Dominosteine.
>
> Das Land versinkt in Dunkelheit. In allen Häusern und Geschäften gehen die Lichter aus. Flughäfen, Krankenhäuser und andere wichtige Einrichtungen schalten fieberhaft auf Notstromaggregate um.
>
> Züge und Aufzüge kommen zum Stehen. Mobilfunkmasten schalten auf Akku- und Notstromversorgung um, doch die Netze sind schnell überlastet und die Netzabdeckung verschlechtert sich zusehends.

> Da Straßen blockiert sind und Tankstellen keinen Treibstoff liefern können, weil die Zapfsäulen Strom benötigen, sind Tausende von Autofahrern gestrandet und verbringen die Nacht in ihren Autos oder am Straßenrand, viele ohne Wasser und unfähig, ihren Angehörigen zu berichten, was passiert.
>
> Am Morgen sind die Straßen voller Menschen, die wissen wollen, was los ist. Das Fehlen von Internet, WLAN und zuverlässigem Mobilfunkempfang verschärft die Verwirrung. Vereinzelt kommt es zu Ausschreitungen, die die Regierung dazu zwingen, den Einsatz des Militärs zu erwägen.
>
> Und das sind nur die ersten 12 Stunden.

Sie beschreibt detailliert die jüngsten Ereignisse in Großbritannien, wo sommerliche Nachfragespitzen zu einem chaotischen Abend führten, als Solarstrom versiegte, der Wind nachließ und mehrere Gaskraftwerke unerwartet den Betrieb einstellten. Die britischen Netzbetreiber mussten die Exporte nach den Niederlanden und Frankreich abrupt stoppen. Sie waren nicht darauf vorbereitet, und das Netz verkraftete die Situation nicht ohne Krisenintervention. Soweit wir wissen, handelte es sich dabei nicht um einen Hackerangriff, sondern einfach um einen warmen Sommertag.

Australien befindet sich in einer ähnlichen Lage wie Großbritannien und ist zunehmend abhängig von fehleranfälliger und unzuverlässiger Ausrüstung, die komplizierte Backup-Systeme erfordert. All dies wird von einer Vielzahl elektronischer Geräte gesteuert, hergestellt von einem Land, das bereit ist, Handelspartner nach Belieben zu sabotieren. Wir sprechen hier von einem Land, das bereitwillig infektiöse Biowaffen in die Welt hinausschickt, während es sie im eigenen Land einsperrt.

Im Gegensatz zu Australien ist Großbritannien zwar nicht so stark von Solaranlagen und Batteriespeichern betroffen, aber zunehmend auf Seekabel nach Norwegen und Frankreich angewiesen, um etwa ein Sechstel seines Strombedarfs zu decken – beide Länder haben Schwierigkeiten, ihre nationalen Stromnetze zu versorgen. China wurde wiederholt beim Durchtrennen von Kabeln um Taiwan ertappt und könnte dies vermutlich auch in der Nordsee tun.

Vor einigen Wochen wurden vor Perth verdächtigerweise zwei Unterseekabel kurz nacheinander und in unmittelbarer Nähe beschädigt. Es handelte sich zwar um Informationskabel, nicht um Stromkabel, doch verdeutlicht der Vorfall das Risiko, sich darauf zu verlassen, dass Länder im Bereich der Meeresumwelt friedlich zusammenarbeiten.

Mit freundlicher Genehmigung von John Connor II

https://joannenova.com.au/2026/09/iran-shuts-down-a-uk-power-plant-for-four-days-but-thats-no-biggie/

Zum Thema

Nahe Kraftwerk Jänschwalde
Sprengvorrichtung an Umspannwerk in Brandenburg gefunden

Stand: 01.09.2026 • 17:44 Uhr

In Brandenburg sind in der Nähe des Kraftwerks Jänschwalde Sprengvorrichtungen gefunden worden. Laut Ministerpräsident Woidke war es ein „Anschlagsversuch“ auf die Stromversorgung. Die Hintergründe sind noch unklar.

https://www.tagesschau.de/inland/sprengvorrichtung-umspannwerk-brandenburg-100.html

Anschlag in Bergheim: Was ist überhaupt ein Umspannwerk?

Stand: 02.09.2026, 17:17 Uhr

Der Anschlag auf ein Umspannwerk in Bergheim sorgt für Aufregung – und für viele Fragen. Wie funktioniert ein Umspannwerk überhaupt und wie sicher ist unsere Stromversorgung?

https://www1.wdr.de/wirtschaft/anschlag-umspannwerk-stromversorgung-sicherheit-100.html

- Ist das ein neues Hobby?