Sicherheitsexperten sind besorgt über mögliche Schäden, die Elektroauto-Batterien anrichten können.

geschrieben von Chris Frey | 6. April 2026

Ronald Stein

Mit Dr. Michael Hogan

Experten für Cybersicherheit und nationale Sicherheit haben untersucht, wie Batterien von Elektrofahrzeugen und die damit verbundene Technologie für terroristische Anschläge oder Aktionen verärgerter Mitarbeiter missbraucht werden könnten, um Störungen oder Massenopfer zu verursachen.

EV-Batterien bergen inhärente Gefahren (brennbare Elektrolyte, Explosions- und Brandgefahr bei Missbrauch), die für böswillige Handlungen ausgenutzt werden könnten. Die größte Sorge der Experten für Cybersicherheit und nationale Sicherheit gilt der Möglichkeit, dass EV-Batterien als Komponenten für einen neuartigen, groß angelegten Terroranschlag unter Verwendung bestehender Technologien eingesetzt werden könnten.

Der gewaltige Brand einer Lithium-Ionen-Batteriefabrik in Moss Landing im Januar 2025 hat die unbekannten Risiken von Explosionen in diesen Fabriken offenbart. Der Physiker und Vorstandsvorsitzende des California Arts and Sciences Institute Dr. Hogan erläuterte in seinem Interview mit Epoch Times mit dem Titel [übersetzt] „Die unbekannten Risiken von Explosionen in Batteriefabriken in Kalifornien“ die Folgen für die Menschen und die Umgebung, die noch lange nach dem Ereignis selbst spürbar sind.

Zum größten Meeresverschmutzungs-Ereignis der Weltgeschichte war es vor einigen Jahren auf den Azoren gekommen.

Sowohl Matson als auch Alaska Marine Lines haben als Reaktion auf die zunehmenden Brandrisiken im Zusammenhang mit dem Transport von Elektrofahrzeugen erhebliche Änderungen an ihren Beförderungsbedingungen vorgenommen. Sie haben entweder die Annahme neuer Buchungen ausgesetzt oder die Beförderung von Elektrofahrzeugen an Bord ihrer Schiffe gänzlich eingestellt.

Was Cybersecurity-Experten bereits wissen

Diese Sicherheitslücken sind keine theoretische Gefahr.

Batteriemanagementsysteme steuern kritische Funktionen: Temperaturregelung, Laderaten, Zellausgleich und Stromverteilung. Werden diese Systeme manipuliert, kann dies zu thermischen Ausbrüchen führen, Fahrzeuge aus der Ferne außer Betrieb setzen oder durch Manipulation der Ladeverläufe lokale Stromnetze destabilisieren.

Analysten für nationale Sicherheit wissen etwas, was dem Durchschnittsverbraucher nicht bewusst ist: **Die Größenordnung spielt eine entscheidende Rolle.**

[Hervorhebung im Original]

Ein einzelnes betroffenes Fahrzeug ist eine Unannehmlichkeit. Zehntausend betroffene Fahrzeuge, die im Rahmen eines koordinierten Angriffs gleichzeitig aufgeladen werden, werden zu einer Bedrohung für die Netzstabilität. Wenn man Millionen von Elektrofahrzeugen in bestimmten geografischen Gebieten konzentriert – Kalifornien, große Ballungsräume, wohlhabende Küstenstädte –, schafft man konzentrierte Schwachstellen.

Die gleichen Politiker, die aggressive Vorschriften für Elektrofahrzeuge vorantreiben, sprechen diese Risiken selten öffentlich an. Sie preisen die ökologischen Vorteile an, schweigen aber über die Cybersicherheits-Infrastruktur, die zum Schutz der vernetzten Fahrzeugnetze erforderlich ist.

Das ist keine Energiekompetenz. Das ist selektive Information, die Verbraucher Risiken aussetzt, von denen sie nichts verstehen.

Das Problem in der Lieferkette, über das niemand sprechen will

Was die Sache noch schlimmer macht: **Wir haben keine Kontrolle über die Lieferkette.** Die Elektrofahrzeuge antreibenden Batterien sind auf Materialien und Herstellungsverfahren angewiesen, die von anderen Ländern dominiert werden. Lithium, Kobalt, Nickel und Seltenerdmetalle – der Großteil davon stammt aus Ländern, die nicht die Interessen der USA teilen.

[Hervorhebung im Original]

China kontrolliert etwa 80 % der weltweiten Produktion von Batteriezellen. Wenn die nationale Verkehrsinfrastruktur von Komponenten abhängt, die von potenziellen Gegnern hergestellt werden, entsteht eine strategische Schwachstelle, die über einfache Cybersicherheit hinausgeht.

Die Frage ist nicht, ob diese Schwachstellen existieren. Die Frage ist, ob wir die defensive Infrastruktur aufbauen, um uns davor zu schützen, bevor eine flächendeckende Einführung das Problem unlösbar macht. Derzeit tun wir das nicht.

Fragen, die Führungskräfte beantworten sollten

Bevor wir eine flächendeckende Einführung von Elektrofahrzeugen vorschreiben, müssen die politischen Entscheidungsträger grundlegende Fragen beantworten, die Cybersicherheitsexperten seit Jahren stellen:

• Wie schützt man Millionen vernetzter Fahrzeuge vor koordinierten Cyberangriffen?

• Was passiert, wenn böswillige Akteure gleichzeitig die Batteriemanagementsysteme von Tausenden von Fahrzeugen manipulieren?

• Wie sichert man ein dezentrales Energiespeichernetz, das ganze Regionen umfasst?

• Welche Sicherheitsvorkehrungen verhindern, dass im Ausland hergestellte Komponenten Hintertüren oder Schwachstellen enthalten?

• Wie reagiert man, wenn die Netzstabilität von Fahrzeugbatterien abhängt, die aus der Ferne manipuliert werden können?

• Das sind keine rhetorischen Fragen. Es gibt technische und sicherheitsrelevante Herausforderungen, die konkrete Antworten erfordern, bevor wir unsere nationale Infrastruktur auf eine Technologie setzen, die wir noch nicht vollständig gesichert haben.

• Das Schweigen der politischen Entscheidungsträger zu diesen Themen sagt alles darüber aus, welche Prioritäten sie setzen.

Energiekompetenz umfasst auch Sicherheitskompetenz

Echte Energiekompetenz bedeutet, nicht nur zu verstehen, wie Technologie funktioniert, sondern auch, welche Risiken sie mit sich bringt.

Elektrofahrzeuge stellen einen grundlegenden Wandel in der Art und Weise dar, wie wir den Verkehr antreiben. Dieser Wandel bringt sowohl Vorteile als auch Schwachstellen mit sich. Eine ehrliche Bewertung erfordert, beides anzuerkennen.

Die Experten für Cybersicherheit und nationale Sicherheit, die diese Risiken verstehen, sind keine Gegner von Elektrofahrzeugen. Sie setzen sich für Sicherheit ein. Sie fordern, dass in die defensive Infrastruktur genauso viel investiert wird wie in die Fahrzeugproduktion und die Ladenetzwerke. Das ist nicht unangemessen. Das ist grundlegende Sorgfaltspflicht.

Wir können eine Zukunft mit Elektrofahrzeugen gestalten. Aber wir müssen sie auf sicheren Fundamenten aufbauen, mit Lieferketten, die wir kontrollieren, und Sicherheitsprotokollen, die dem Ausmaß der von uns geschaffenen Schwachstellen entsprechen.

Alles andere setzt Millionen von Amerikanern Risiken aus, die sie nicht verstehen: Sie fahren Fahrzeuge, die mit Netzwerken verbunden sind, die sie nicht schützen können, und sind von einer Infrastruktur abhängig, die von böswilligen Akteuren ins Visier genommen werden kann. Das ist die Realität, die Cybersicherheitsexperten bereits kennen. Die Frage ist, ob auch der Rest von uns dies begreifen wird, bevor die Schwachstellen ausgenutzt werden.

Die technischen Herausforderungen sind lösbar. Die Schwachstellen in der Lieferkette können behoben werden. Die Cybersicherheitsprotokolle können entwickelt und umgesetzt werden. Aber nur, wenn wir die Probleme ehrlich anerkennen und in Lösungen investieren, die den Risiken angemessen sind.

Derzeit bauen wir ein Verkehrssystem auf Fundamenten, die wir nicht gesichert haben. Das ist kein Fortschritt. Das ist Fahrlässigkeit, die sich als Innovation tarnt.

This article originally appeared at America Out Loud

Link: https://www.cfact.org/2026/03/28/security-experts-concerned-by-potential-ev-battery-harm/

Übersetzt von Christian Freuer für das EIKE

Anmerkung des Übersetzers: Was in dem Beitrag mit keinem Wort angesprochen wird: Natürlich kosten diese erforderlichen Sicherheitsmaßnahmen Geld – und vermutlich viel Geld, zusätzlich zu der ohnehin schon mega-teuren EV-Wirtschaft.