Energiebranche wappnet sich gegen Drohnen

- 26.10.2026
- Neue Zürcher Zeitung
- David Vonplon

Über dem Stern von Laufenburg tauchte vergangenen Herbst eine Drohne auf. Mehrere Personen sichteten ein Flugobjekt mit einem Durchmesser von zweieinhalb Metern - und hegten einen bösen Verdacht: Wird hier, an diesem neuralgischen Punkt des europäischen Stromnetzes, ein Angriff vorbereitet? An der Schaltanlage im Aargau treffen die Stromnetze der Schweiz, Deutschlands und Frankreichs aufeinander. Ein schwerer Schaden könnte im Extremfall Millionen Menschen im In- und Ausland von der Stromversorgung abschneiden. Ein paar Wochen später folgte dann die Entwarnung: Hinter den Flügen steckte eine Firma, die Leitungen inspizierte. Die Betreiberin Swissgrid hatte die Flüge bewilligt.

Was nach einer möglichen Spionageaktion aussah, diente dem Unterhalt des Netzes. Doch die harmlose Erklärung für Laufenburg schafft das grundsätzliche Problem nicht aus der Welt. Dazu genügt ein Blick ins umliegende Ausland: Am Flughafen Leipzig gab es im August einen Anschlagsversuch mit sprengstoffbeladenen Drohnen. Im September wurden auch Umspannwerke und Hochspannungsleitungen in Nordrhein-Westfalen zum Ziel von Sabotageakten. Solche Angriffe sind in der Schweiz auch möglich.

Schwer erkennbare Bedrohung Die Schweizer Behörden sehen Anlass zu erhöhter Wachsamkeit. Hierzulande sei «eine Zunahme von Drohnenflügen über militärischen und kritischen Infrastrukturen festzustellen», hielt das Verteidigungsdepartement unlängst fest. Entsprechende Sabotageaktionen sind in der Schweiz bis jetzt zwar nicht bekannt. Der Bundesrat warnt jedoch davor, dass ein staatlicher Akteur kritische Infrastruktur in der Schweiz angreifen könnte, um davon abhängige Staaten oder Bündnisse zu treffen. Für Energieversorger und Sicherheitsbehörden stellt sich damit immer dringlicher die Frage: Wie lassen sich Kraftwerke und Stromnetze gegen eine Bedrohung schützen, die oft erst erkennbar wird, wenn sie bereits über der Anlage schwebt? Schon bei der Erfassung der Gefahr gibt es Lücken.

«Die Bedrohungslage ist für die Betreiber nicht einfach zu interpretieren», sagt Ivo Capaul vom Center for Security Studies der ETH Zürich. Die wenigsten von ihnen hätten Sensoren zur Erkennung von Drohnen an ihren Anlagen installiert. Mit blossem Auge lasse sich teilweise kaum feststellen, ob überhaupt eine Drohne unterwegs sei. Umso wichtiger sei es, dass die Betreiber von kritischen Infrastrukturen entsprechende Systeme installierten. Allein auf Polizei und Armee können sich die Betreiber nicht verlassen.

«Ein permanenter Schutz durch staatliche Behörden ist nicht realistisch», sagt Capaul. Aktive Drohnenabwehrsysteme seien teuer, technisch komplex und schützten nur einen begrenzten Umkreis. Selbst mit mehreren Systemen liesse sich deshalb nur ein Bruchteil der kritischen Infrastrukturen abdecken. Zudem müsste die Abwehr bereits vor Ort einsatzbereit sein, bevor eine Drohne auftauche. Die Betreiber müssten deshalb auch selber vorsorgen, sagt Capaul.

«Häufig ist der passive Schutz die zweckdienlichere Lösung.» Verwundbare Anlagenteile liessen sich etwa durch bauliche Vorkehrungen oder Netze schützen, heikle Bereiche gegen Spionage abschirmen. Welche Massnahmen nötig seien, wüssten die Unternehmen am besten. Entscheidend sei zudem die Fähigkeit, nach einem Vorfall möglichst rasch wieder zum Normalbetrieb zurückzukehren. Doch bei dieser Vorsorge gibt es Nachholbedarf.

«Der physische Schutz dieser Anlagen gegen Vandalismus, Terroranschläge oder Drohnenangriffe ist nicht überall genügend umgesetzt», sagt Ronny Kaufmann, Chef von Swisspower, einer Allianz von zwanzig Stadtwerken und anderen Energieversorgern. Investiert werden müsse vor allem dort, wo ein Ausfall schwerwiegende und länger anhaltende Folgen

hätte. Neben baulichen Schutzmassnahmen brauche es geschulte Mitarbeitende, klare Alarmierungswege und rasch verfügbares Ersatzmaterial. Sichtschutzplanen und Netze Bereits auf die Bedrohungslage reagiert hat der Baselbieter Energieversorger Primeo, der rund eine halbe Million Menschen mit Strom versorgt. Bei seinen 24 Unterwerken hat das Unternehmen Sichtschutzplanen installiert, damit die Anlagen von aussen nicht einsehbar sind.

Auch Gitterabsperrungen sind vorhanden. Zudem plant Primeo, Schutznetze gegen Drohnen über die Anlagen zu spannen, wie zuerst das Portal «Prime News» berichtete. Insgesamt investiert das Unternehmen rund eine Million Franken in entsprechende Schutzmassnahmen. Auch Swissgrid, die für den sicheren Betrieb des Schweizer Übertragungsnetzes verantwortlich ist, verstärkt derzeit den Schutz ihrer Anlagen vor Drohnen. «Wir aktualisieren unsere Bedrohungsanalyse laufend und stehen mit anderen Betreibern kritischer Infrastrukturen in der Schweiz und in Europa im Austausch», sagt der Sprecher Noël Graber.

Dem Vernehmen nach reichen die Kontakte dabei bis in die baltischen Staaten und die Ukraine. Um die eigenen Unterwerke hat Swissgrid Flugverbotszonen eingerichtet. Eine virtuelle Sperre in der Software verhindert an diesen Knotenpunkten den Einflug handelsüblicher Drohnen. Gemeinsam mit den Behörden testet Swissgrid zudem verschiedene Systeme zur Identifikation und Abwehr von Drohnen. Die Beschaffung von Detektionssystemen dürfte in den kommenden Monaten folgen.

Parallel wird geprüft, wo zusätzliche Investitionen in den physischen Schutz sinnvoll sind. Dabei muss auch Swissgrid Prioritäten setzen: Das weitläufige Netz lässt sich kaum überall gleich stark sichern. Swissgrid betreibt das Netz so, dass es auch beim Ausfall einzelner Elemente stabil bleibt. Einzelne beschädigte Elemente müssen deshalb nicht zu einem Versorgungsunterbruch führen. Kommt es dennoch zu einer Störung, zählt die rasche Wiederherstellung.

Dafür sind verfügbare Ersatzteile und Materiallager zentral. Schäden an Freileitungen lassen sich damit vergleichsweise schnell beheben. Die Vorsorge hat allerdings Grenzen. Werden einzelne Elemente beschädigt, kann ein entsprechend ausgelegtes Netz den Ausfall auffangen. Ein koordinierter staatlicher Angriff stellt dagegen Anforderungen, welche die Möglichkeiten einer Netzbetreiberin übersteigen.

In solchen Fällen braucht es staatliche Unterstützung, insbesondere durch Polizei und Armee. Swissgrid begrüsst deshalb, dass die potenzielle Gefährdung kritischer Infrastrukturen durch Drohnen mehr politische Aufmerksamkeit erhält. Das Grundproblem bleibt jedoch: Identifiziert ein Netzbetreiber verdächtige Drohnen über seinen Anlagen, darf er diese nicht selbst bekämpfen, sondern muss die Polizei alarmieren. Bis diese eintrifft, ist die Drohne womöglich längst verschwunden. Auch eingeübte Abläufe beseitigen diesen Zeitverlust nicht.

Hinzu kommt, dass nicht klar geregelt ist, welche Stelle bei Angriffen unterhalb der Kriegsschwelle für die Bekämpfung der Drohnen zuständig ist und wer die Koordination übernimmt: die Polizei, die Kantone, das Bundesamt für Zivilluftfahrt, Skyguide oder die Armee. Die Sicherheitspolitische Kommission des Ständerats sprach diesbezüglich unlängst gar von einem «Zuständigkeitschaos». Eine mittlerweile von beiden Kammern gutgeheissene Motion fordert den Bundesrat auf, Klarheit zu schaffen. Bewaffnete Stromanbieter? Noch einen Schritt weitergehen will der SVP-Nationalrat Thomas Hurter. Er sagt: «In der Schweiz häufen sich die Drohnensichtungen über Flughäfen, Militäranlagen und Energieinfrastrukturen.

Zivile Betreiber bleiben jedoch schutzlos.» Der Schaffhauser Politiker fordert deshalb in einem Vorstoss, dass die Betreiber kritischer Infrastrukturen bei akuter Bedrohung durch Drohnen eigenständig Abwehrmassnahmen ergreifen dürften. Dazu könnten Störsender gehören, welche die Funkverbindung zur Drohne unterbrechen, Abfangdrohnen, die sie mit Netzen einfangen, oder als letztes Mittel der Abschuss mit einer Schusswaffe. Sollen also Netzbetreiber und Energieversorger bald bewaffnet werden? Der Verband der Schweizer Elektrizitätsunternehmen will sich dazu nicht äussern. Für ihn steht im Zentrum, dass im Ernstfall keine Zeit mit Kompetenzfragen verlorengeht.

«Die Zuständigkeiten zwischen Betreibern, Polizei und Behörden müssen klar geregelt sein»,

sagt die Sprecherin Irit Mandel. Gerade bei besonders kritischen Anlagen wie Kraftwerken oder Unterwerken müssten alle Beteiligten rasch handlungsfähig sein. Einen lückenlosen physischen Schutz hält der Verband ohnehin nicht für möglich: Einzelne Schlüsselanlagen könnten gezielt gesichert werden, das weitverzweigte Stromnetz dagegen kaum. Umso wichtiger seien robuste und redundante Netze sowie klare Abläufe, damit beschädigte Anlagen möglichst rasch wieder in Betrieb genommen werden könnten. Der Swisspower-Chef Kaufmann unterstützt die Stossrichtung von Hurters Vorstoss, beharrt aber auf dem staatlichen Gewaltmonopol.

«Dass ein Stadtwerk eine militärische Drohne vom Himmel holt, erachte ich als nicht realistisch.» Auch der Bund räumt derweil erhebliche Lücken ein: «Die Schweiz verfügt gegenwärtig nicht über ausreichende Fähigkeiten, um den Schutz und die Abwehr gegen Drohnen in grösserem geografischem Ausmass zu gewährleisten», sagt Brigitte Mader, Sprecherin des Bundesamtes für Energie. Ein flächendeckender Schutz des Stromnetzes sei nicht möglich. Die Schutzmassnahmen müssten sich deshalb nach den jeweiligen Risiken richten. An der geltenden Aufgabenteilung hält das Amt fest: Die Betreiber seien für die Sicherheit ihrer Anlagen verantwortlich, Zwangsmassnahmen blieben jedoch den staatlichen Behörden vorbehalten.

Ab einer gewissen Bedrohungslage müssten die Unternehmen über die kantonalen Behörden polizeiliche oder subsidiär militärische Unterstützung beantragen. Mader weist indes darauf hin, dass die Stellen des Bundes und der Kantone derzeit unter Leitung des Sicherheitsverbunds Schweiz prüften, wie sich die Erkennung und Abwehr von Drohnen verbessern liessen. «Davon werden letztlich auch die Betreiber kritischer Infrastrukturen profitieren», sagt sie. Sicher ist: Der Handlungsbedarf ist beträchtlich. Heute mangle es nicht nur vielerorts an geeigneten Überwachungssystemen und klaren Abläufen für eine wirksame Drohnenabwehr, sagt Kaufmann.

Auch fehle eine zentrale Meldestelle für Drohnensichtungen. Die Unternehmen leisteten ihren Beitrag zum Schutz der Anlagen und zur Aufrechterhaltung der Versorgung. «Dafür brauchen sie aber einen handlungsfähigen staatlichen Partner.» Der Stern von Laufenburg ist nicht nur für die Schweizer Stromversorgung von grosser Bedeutung. GAËTAN BALLY / KEYSTONE Thomas Hurter Nationalrat, SVP Ivo Capaul Researcher, ETH Zürich KEYSTONE, ETH Es ist nicht klar geregelt, welche Stelle bei Angriffen unterhalb der Kriegsschwelle für die Bekämpfung der Drohnen zuständig ist.