LUFTSICHERHEIT

DROHNEN auf Abwegen

Um Kosten zu sparen, erwägen viele Unternehmen den Einsatz unbemannter Flugkörper. Doch die Risiken für die Luftfahrt sind erheblich.

Von Todd Humphreys und Kyle Wesson

Während Friedensforscher diskutieren, welche Auswirkungen ferngesteuerte oder gar autonome Drohnen auf Kriegsbereitschaft und Kriegsführung haben können, gewinnt die Drohnentechnik neue Anhänger im zivilen Bereich. Die Bundesluftfahrtbehörde der Vereinigten Staaten (FAA) schätzt, dass bis zum Jahr 2030 mehr als 10 000 unbemannte Flugkörper ihre Bahnen am amerikanischen Himmel ziehen werden: um Such- und Rettungsaktionen zu unterstützen, die Bestäubung landwirtschaftlicher Nutzflächen zu erledigen, Stromleitungen zu überwachen, Messungen vorzunehmen und vieles mehr. Frederick W. Smith, Gründer des Paketdienstes FedEx, erwog, Luftfracht mit Drohnen zu befördern, Amazon-Chef Jeff Bezos will sogar Päckchen und Pakete mit Minihubschraubern zum Kunden bringen.

Der Reiz besteht vor allem in der Wirtschaftlichkeit der Geräte: kein Cockpit, weniger Personalkosten. Nur ein Bediener am Boden, der die Flugroute in einen Computer eingibt, die Drohne mit einer Art Joystick steuert – und über weite Strecken dem Autopiloten die Steuerung überlässt. Der amerikanische Kongress wies deshalb die Luftfahrtbehörde an, bis 2015 einen umfassenden Plan vorzulegen, wie sich zivile unbemannte Flugkörper in das nationale Flugsicherheitssystem einbeziehen ließen.

Doch das dürfte alles andere als einfach werden, denn die Drohnentechnik hat erhebliche Schwachstellen, wie ein Vor-

Sieht so die Zukunft aus? Eine Vielzahl ziviler unbemannter Flugkörper schwirrt durch den Luftraum unserer Städte? Mögliche Anwendungen gibt es genug: Sie reichen von Paketzustellung über Umweltmessungen bis zur Videoüberwachung. Allerdings sind zahlreiche Fragen offen. Diese betreffen nicht nur den Schutz der Privatsphäre, sondern mehr noch die Luftsicherheit.

SHUTTERSTOCK / ANDREA CRISANTE

PICTURE ALLIANCE / AP PHOTO / EDUARDO CONTRERAS

fall vom 2. August 2010 illustriert. Auf Grund eines Softwareproblems, so die späteren Ermittlungen, verirrte sich eine MQ-8B Fire Scout (siehe Fotos) weit in den Luftraum über der Hauptstadt Washington, in dem auch das Präsidentenflugzeug Air Force One operiert. Die 1429 Kilogramm schwere und 9,7 Meter lange Drohne der US-Navy flog dort ohne Verbindung zu seinen Bedienern im Kontrollraum von Maryland und führte obendrein die für einen solchen Notfall programmierte Anweisung nicht aus, umgehend zur Basis zurückzukehren. Erst nach einer halben Stunde, in der die Nerven blank lagen, gelang es der Crew, die Kommunikation wieder aufzubauen und die Drohne zu steuern. Immerhin, so betonte ein Vertreter der Navy, hatte der Autopilot dafür gesorgt, dass sie in der Zwischenzeit ihre Flughöhe konstant hielt.

Tatsächlich birgt die Kommunikation mit Drohnen ein erhebliches Sicherheitsrisiko. Die Flugkörper errechnen ihre Position im Raum anhand der Signale von GPS-Satelliten und senden ihrerseits anderen Luftfahrzeugen Informationen. Die eigentliche Steuerung erfolgt über eine Verbindung zur Bodenstation. Fällt einer dieser Kanäle aus, kann das katastrophale Folgen zeitigen.

Schwachstelle GPS-Signal

Das GPS wird ergänzt von Sensoren für die Trägheitsnavigation, Magnetfeldstärken- und Höhenmessgeräten sowie Kameras. Dennoch bleibt der GPS-Empfänger das zentrale Element der Ortsbestimmung, da er im Gegensatz zu allen anderen Geräten auch nachts und bei schlechten Wetterbedingungen hochpräzise Daten liefert.

Drohnen für zivile Anwendungen werden aber die frei zugänglichen und unverschlüsselten GPS-Signale verwenden, wie es beispielsweise auch Autonavigationssysteme tun. Leider enthalten diese Daten keinerlei Authentisierung. Die erste Gefahr ist daher das so genannte Spoofing: Ein gefälschtes Signal überdeckt das echte. Wie das möglich ist, demonstrierte unser Labor im Juni 2012 im White Sands Missile Range in New Mexiko. Aus gut 500 Meter Entfernung manipulierten wir den Autopiloten einer 80 000-Dollar-Drohne. Unser Spoofer sandte eine leicht veränderte, dabei aber in der In-

AUF EINEN BLICK

FALSCHE SIGNALE

1 Von Überwachungsaufgaben bis zur Paketauslieferung reichen die Ideen für den **zivilen Einsatz von Drohnen**. Schätzungen zufolge könnten im Jahr 2030 mehr als 10 000 davon in den USA im Einsatz sein.

2 Für die Sicherheit des Luftverkehrs bergen unbemannte Flugkörper zahlreiche Probleme, die bislang nur unzureichend bedacht wurden. Diese betreffen die **Kollisionsvermeidung** wie auch die **Sicherheit gegen Angriffe und Entführungen**.

3 Die zur Positionsbestimmung ausgewerteten Signale von **GPS-Satelliten** können gestört oder verfälscht werden, Gleiches gilt für die Kommunikation mit anderen Luftfahrzeugen via **ADS-B-Transponder**. Eine Lösung ist derzeit nicht in Sicht.

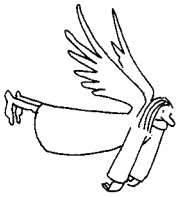
US NAVY PHOTO BY MASS COMMUNICATION SPECIALIST 2ND CLASS ALAN GRAGG

Die MQ-8 Fire Scout (hier in der Version MQ-8B) ist ein unbemannter Hubschrauber der amerikanischen Marine. Die Drohne kann autonom starten und landen – auch in unbekanntem Gelände. Neben einer Videoeinheit trägt sie bei Aufklärungsflügen im Turm verschiedene Sensorsysteme, etwa zur Entfernungsmessung per Laser, Radarüberwachung oder zum Abhören der Kommunikation des Gegners. Sie lässt sich aber auch mit Lenkwaffen ausrüsten. 2010 geriet ein solches System über Washington außer Kontrolle und reagierte eine halbe Stunde lang auf keinen Fernbefehl der Leitstelle.

tensität stärkere Version des korrekten GPS-Signals. Weil die Software zwischen Original und Fälschung nicht unterscheiden konnte, steuerte der Autopilot auf Grund falscher Höhenangaben in Richtung Wüstenboden, bis der Bediener auf manuelle Kontrolle umstellte und das Gerät quasi auf Sicht rettete.

Wie gefährlich Spoofing sein kann, ist mindestens seit 2001 bekannt, wurde aber bis vor Kurzem von Politikern und GPS-Herstellern weit gehend ignoriert. Ein Angriff galt wohl als unwahrscheinlich. Die Konsequenz: Es wird Jahre dauern, geeignete Verschlüsselungsverfahren und eine digitale Signatur zu entwickeln, die für Ursprung und Inhalt der Signale bürgt.

Ein gezielter Angriff könnte sogar noch weit simpler aussehen. Nahe der Erdoberfläche sind die Satellitensignale nämlich sehr schwach, vergleichbar dem Licht einer 50-Watt-Glühbirne in einer Entfernung von 22 000 Kilometern. Es würde genügen, ein Rauschen im Frequenzbereich des GPS-Signals auszustrahlen, um den Empfang zu stören. Im Mai 2012 verlor in Südkorea das Steuerungspersonal die Kontrol-



le über eine 150 Kilogramm schwere Aufklärungsdrohne. Sie krachte in ihre Bodenstation, tötete einen Ingenieur und verletzte zwei Bediener. Die Rekonstruktion der Ereignisse ergab, dass Störsignale aus Nordkorea eine Kettenreaktion in Gang gesetzt hatten.

Drohnen sind Fluggeräte, die mit Helikoptern und Kleinflugzeugen zusammenstoßen könnten, im Bereich der Start- und Landerouten von Flughäfen auch mit Verkehrs- und Transportflugzeugen. Piloten beobachten immerhin noch ihre Umgebung und verwenden Radar, um Kollisionsgefahren zu erkennen. Doch wie der US-Rechnungshof in einem Bericht 2012 schrieb: »Es gibt noch keine geeignete Technologie, die unbemannte Flugkörper dazu in die Lage versetzt, andere Flugzeuge und Luftfahrzeuge zu erkennen.«

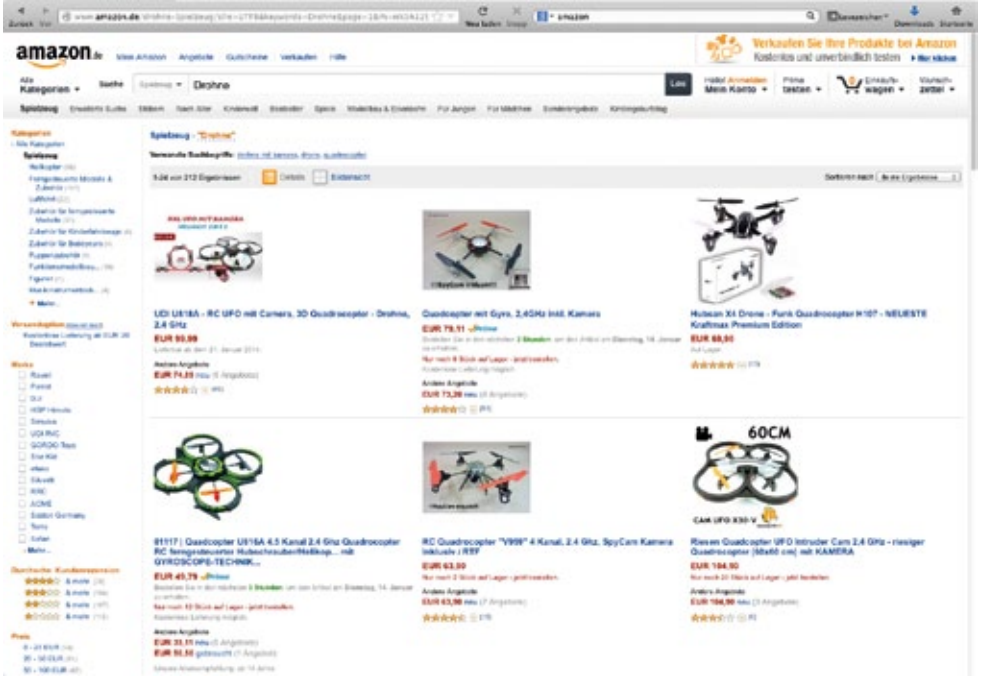
Radarsysteme kommen nicht in Frage – sie sind zu groß und energiehungrig. Kameras für sichtbares und infrarotes Licht wären eine preisgünstige Alternative, können aber nicht durch Wolken schauen. Die Lösung dürfte Automatic Dependent Surveillance-Broadcast (ADS-B) heißen. Ein ADS-B-Transponder an Bord eines Flugzeugs meldet sekündlich Position und Geschwindigkeit; umgekehrt empfängt er die Daten anderer Flugzeuge. Die Bundesluftfahrtbehörde der USA will, dass bis 2020 alle zugelassenen Flugzeuge, unabhängig von ihrer Größe, mit ADS-B ausgestattet werden. Auch das Projekt, den europäischen Luftraum hinsichtlich der Flugsicherung zu vereinheitlichen (Single-European-Sky) setzt auf ADS-B. Bis 2019 sollen alle Flugzeuge damit ausgerüstet sein – ausgenommen leichte und langsame, was die Einbeziehung ziviler Drohnen in die Luftraumüberwachung hier zu Lande problematisch macht.

Unabhängig davon lässt sich ein ADS-B-Transponder in der gleichen Manier täuschen wie ein GPS-Empfänger. Als diese Technik in den 1990er Jahren entwickelt wurde, spielten Sicherheitsfragen kaum eine Rolle. 2012 demonstrierten Forscher vom Air Force Institute of Technology in Ohio, dass falsche Signale sehr leicht programmiert und mit einfachen technischen Mitteln versendet werden können. Während ein Pilot anhand des Radars den Betrug noch entdecken und einen Kollisionskurs korrigieren könnte, verfügt eine Drohne über kein vergleichbares Kontrollinstrument.

Im Notfall: Rückkehr zur Basis

Drohnen werden vom Bediener über eine Command-and-Control-Funkverbindung gesteuert. Zwar gibt es dafür sichere Kommunikationsprotokolle, doch die schützen nicht vor einem Angriff, der das Signal stört. Für eine abgebrochene Verbindung gibt es bisher keine zufrieden stellende Lösung. Üblicherweise programmiert man Anweisungen ein, zum Beispiel die, zur Ausgangsbasis zurückzukehren, falls die Verbindung länger als 30 Sekunden abreißt. Doch das funktioniert nur, wenn Navigation und Steuerung ansonsten ordentlich arbeiten. Im Übrigen muss die Störung der Command-and-Control-Signale nicht einmal gezielt herbeigeführt werden: Da es kaum noch unbesetzte Funkkanäle gibt, kommunizieren Drohnen auf frei zugänglichen Frequenzen mit dem Kontrollzentrum – und können leicht einmal Daten aufschnappen, die gar nicht an sie gerichtet waren.

Sicherheit im Luftverkehr wird in den USA wie in Europa großgeschrieben. Deshalb genehmigen die Behörden auf beiden Seiten des Atlantiks neue Technologien nur nach intensiver Prüfung, ob sie die Flugsicherheit beeinträchtigen könnten. Sie stehen nun vor der Herausforderung, Vorschriften für den Betrieb von Drohnen entwickeln zu müssen, während ihnen gleichzeitig Modernisierungsaufgaben ins Haus stehen, da viele Radaranlagen in die Jahre gekom-



Luftaufnahmen per ferngesteuertem Quadkopter sind bei Videofilmern beliebt. Die mit Kameras bestückten Fluggeräte sind im Internet erhältlich. Doch vor dem Einsatz sollten die rechtlichen Rahmenbedingungen abgeklärt werden. So ist hier zu Lande der Sichtkontakt des Bedieners zur Drohne vorgeschrieben.

DPA / OLIVER BERG

Rotierender Paketbote: Logistikunternehmen wie DHL und der Versandhandelsriese Amazon erproben bereits die Zustellung via Drohne. Manche Fachleute sehr darin allerdings vor allem einen Marketinggag, denn bislang verbietet allein schon die Rechtslage in Deutschland den Einsatz eines zivilen, autonom agierenden Flugkörpers.

men sind und erneuert oder durch eine Technik wie GPS und ADS-B ersetzt werden müssen. Sicherheit darf zudem nicht die wirtschaftlichen Vorteile der Drohnen zunichtemachen. Beispielsweise muss ein unbemannter Flugkörper in Deutschland stets in Sichtweite des Bedieners fliegen, was ihn für viele Zwecke wertlos macht. Auch mit dem Thema Privatsphäre und Datenschutz müssen sich die Luftfahrtbehörden beschäftigen: Wenn eine Drohne über private Grundstücke fliegt, sehen ihre Kameras – und damit auch die steuernde Person – Dinge, die nicht für die Öffentlichkeit bestimmt sind.

41 der 50 Bundesstaaten der USA wollen die Verwendung von Drohnen daher einschränken. Wer von einem unbemannten Flugkörper aus ohne ausdrückliche Zustimmung des Eigentümers Bilder von Privatgrundstücken macht, begeht in Texas eine Ordnungswidrigkeit. Auch in Deutschland kann ein Grundbesitzer solche Eingriffe in seine Privatsphäre untersagen, zudem könnten Urheberrechte von Architekten verletzt werden. Die technischen und regulativen Anforderungen werden die Einführung der Drohnentechnologie vermutlich bremsen, aber wohl kaum stoppen. Bleibt zu hoffen, dass die Zeit reicht, ihre Anfälligkeit gegen unbeabsichtigte Störungen, kriminelle oder gar terroristische Angriffe zu beheben. ~

DIE AUTOREN


Todd Humphreys (links) leitet das Radionavigation Laboratory der University of Texas in Austin, in dem neue Technologien zur Satellitennavigation entwickelt werden. **Kyle Wesson** promoviert dort.

QUELLEN

U.S. Government Accountability Office: Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System, 18. 9. 2012, online unter: www.gao.gov/products/GAO-12-981

Wells, B. C.: Unmanned at Any Speed: Bringing Drones into Our National Airspace. In: Issues in Governance Studies series 55, S. 1–20, 2012. Kostenlos im Internet erhältlich: www.brookings.edu/research/papers/2012/12/14-drones-bennett

WEBLINKS

www.ScientificAmerican.com/nov2013/hacked
Das Online-Video von »Scientific American« zeigt, wie eine Drohne in New Mexico gehackt wird.

Dieser Artikel im Internet: www.spektrum.de/artikel/1221333