HOW TO HACK A DRONE

INHALT

Wie funktioniert eine Drohne

Umgangssprachlich wird der Begriff „Drohne“ oft verwendet, wobei damit in den allermeisten Fällen von Multicoptern die Rede ist. Multicopter sind Flugzeuge, welche mit mehreren Propellern auf der gleichen Ebene ausgestattet sind. Dabei drehen sich jeweils zwei Rotoren in gegenseitiger Richtung, wobei sich deren Drehmoment aufhebt. Somit kann auf einen Heckrotor wie z.B. bei einem Helikopter verzichtet werden. Gesteuert werden Multicopter durch Anpassung der Geschwindigkeit der einzelnen Rotoren. Werden beispielsweise die beiden hinteren Rotoren schneller angetrieben, dann steigt die Drohne hinten stärker an und kippt nach vorne, wobei die Rotoren nun alle nach hinten gerichtet sind und ein Vorwärtsschub entsteht. Das Gleiche gilt für die beiden seitlichen Rotoren für eine Seitwärtsbewegung. Eine Drehung entlang der Z-Achse kann bewirkt werden, indem die zum Beispiel im Uhrzeigersinn drehenden Rotoren schneller drehen. Die beiden Drehmomente der Propeller sind jetzt nicht mehr ausgeglichen und es entsteht eine Drehung der ganzen Drohne im Uhrzeigersinn.

Sensoren

Beschleunigungs- und Lagesensor

Der wohl wichtigste Sensor zur Stabilisierung einer Drohne ist der Lage- und Beschleunigungssensor. Dieser prüft kontinuierlich die Lage gegenüber dem Gravitationszentrum der Erde resp. die Änderung der Beschleunigung. Mittels eines Regelkreises werden nun die Rotoren so angesteuert, dass die Drohne bei Nichteinwirken des Piloten stabil in der Luft steht.

Barometer

Da sich der atmosphärische Luftdruck mit steigender Höhe verkleinert, kann mittels eines Barometers die Höhe der Drohne gemessen werden. Dies hilft zusätzlich der Drohne bei der Neutralstellung des Auf/Abs und wird auch als „Throttle Hebels“ bezeichnet, um sie mit der Fernbedienung, stabil in der Luft zu halten.

Kompass

Ein digitaler Kompass misst das Erdmagnetfeld. Dies hilft eine Drehung, auch „Gieren“ genannt, der Drohne zu verhindern. Zudem dient er zur Orientierung im Raum, was besonders für den automatischen Flugmodus wichtig ist.

GNSS

Besser bekannt unter dem amerikanischen Markennamen „GPS“. Moderne Drohnen nutzen aber meist alle verfügbaren Satelliten, also auch Glonas der Russen, Galileo aus Europa oder Baidu der Chinesen. Das globale Navigationssatellitensystem hilft der Drohne bei zum Beispiel leichtem Wind entgegen zu wirken. Ausserdem ermöglicht es den automatischen Flug.

Automatischer Flugmodus

Mittels Kompass kann sich die Drohne im Raum orientieren und mittels GNSS positionieren. Damit ist es möglich, die Drohne autonom fliegen zu lassen. Hier werden der Drohne Koordinations-Wegpunkte vorgegeben, welche die

Drohne der Reihe nach abfliegt. Damit kann zum Beispiel durch kontinuierliches Auslösen der Kamera an Gelände kartografiert werden.

Rechtliche Grundlagen in der Schweiz

Rechtliche Grundlagen zu Drohnen

In der Schweiz ist das BAZL (Bundesamt für Zivilluftfahrt) für die Aufsicht und Luftfahrtentwicklung verantwortlich. Regelungen betreffend Drohnen werden in der Verordnung des UVEK über Luftfahrzeuge besonderer Kategorien 748.941[1] Abschnitt 7: Unbemannte Luftfahrzeuge bis 30 kg Gewicht geregelt. Dabei gelten folgende Regeln:

Wer ein Modellluftfahrzeug mit einem Gewicht bis zu 30 kg betreibt, muss stets direkten Augenkontakt zum Luftfahrzeug halten und jederzeit die Steuerung gewährleisten können.

Der Betrieb von Modellluftfahrzeugen mit einem Gewicht zwischen 0,5 und 30 kg ist untersagt:

in einem Abstand von weniger als 5 km von den Pisten eines zivilen oder militärischen Flugplatzes;

in aktiven CTR, sofern dabei eine Höhe von 150 m über dem Grund überstiegen wird;

im Umkreis von weniger als 100 Metern um Menschenansammlungen im Freien, es sei denn, es handle sich um öffentliche Flugveranstaltungen nach Artikel 4. [2]

Das BAZL selbst spricht von einer Menschenansammlung ab 24 Personen.

Zusätzlich wird in Artikel 10 vorgeschrieben, dass der Halter einer Drohne einen Haftpflichtnachweis mit einer Garantiesumme von mindestens 1 Million Franken sicherzustellen hat.

Gemeinden sind berechtig zusätzliche Regulierungen für Drohnenpiloten zu erheben, welche man üblicherweise auf deren Webseite findet. Eine Übersicht darüber gibt es leider nicht. Ein Beispiel dafür ist die Gemeinde Augst[3]

Ab Januar 2021 wird die Schweiz die Drohnenregelung der EASA (European Union Aviation Safety Agency) einführen[4]. Diese beinhalten neben weiteren Gewichtsreglementierungen und maximalen Höhenbeschränkungen sowie Distanzregelungen zu Siedlungen zusätzlich eine theoretische Prüfung für den Piloten. Wie diese aber genau in der

[1] https://www.admin.ch/opc/de/classified-compilation/19940351/index.html
[2] Zitat: Verordnung des UVEK über Luftfahrzeuge besonderer Kategorien 748.941
[3] https://www.augustaraurica.ch/fileadmin/user_upload/1_Besuchen/1_Allgemeine_Informationen/Regeln_fur_den_Betrieb_von_Drohnen_und_Flugmodellen_Gemeinde_Augst.pdf
[4] https://www.bazl.admin.ch/bazl/de/home/gutzuwissen/drohnen-und-flugmodelle/Europaeische_Drohnenregulierung_uebernommen.html

Schweiz implementiert werden, ist zum aktuellen Zeitpunkt noch nicht klar. Stand: 04.06.2020 Ursprünglich war der Plan dies bereits auf Juni 2020 einzuführen, dies wurde aber aufgrund der Coronakrise auf Januar 2021 verschoben.

Rechtliche Grundlagen zur Privatsphäre, Kameras an Drohnen

Sind auf den Aufnahmen bestimmte oder bestimmbare Personen ersichtlich, gilt die Datenschutzverordnung[5].

Unter folgendem Link hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte die Regeln zusammen gefasst[6].

Die wichtigsten Punkte dabei sind:

Das Filmen von bestimmbaren Personen mittels Drohne oder anderen Modellluftfahrzeugen darf nur erfolgen, wenn ein Rechtfertigungsgrund vorliegt. Als Rechtfertigungsgrund gilt die Einwilligung der betroffenen Person oder ein überwiegendes privates oder öffentliches Interesse.

Die Videoüberwachung muss für die betroffenen Personen erkennbar sein, sei es durch ein Hinweisschild oder durch eine sichtbare Kamera oder durch vorrangige Information (Transparenzprinzip).

Die Drohnen müssen so eingesetzt werden, dass im Aufnahmefeld der Kamera nur die für den verfolgten Zweck absolut notwendigen Bilder erscheinen (Verhältnismässigkeitsprinzip).

Die Aufnahmen dürfen nur für den ursprünglich geplanten Zweck benutzt werden (Zweckbindungsprinzip). Dabei versteht es sich von selbst, dass Aufnahmen nur gemacht werden dürfen, wenn diese für die Erreichung des Zwecks nötig und geeignet sind. Kann mit anderen, weniger in die Persönlichkeit eingreifenden Mitteln, der gleiche Zweck erreicht werden, ist auf die Aufnahmen zu verzichten (Verhältnismässigkeitsprinzip).[7]

Angriffsszenarien

Angriff auf GNSS

Mittels eines GPS Jammers kann der Drohne die Verbindung zu GPS Satelliten erschwert werden. Diese Geräte sind in der Schweiz offiziell verboten, sind aber trotzdem natürlich im Internet bestellbar[8]. Fliegt die Drohne automatische Wegpunkte ab, ist es für Sie unmöglich, den nächsten Wegpunkt zu finden, zudem kann sie auch den Homepunkt nicht mehr finden. Je nach Modell bleibt sie darum in der Luft stehen oder versucht an Ort und Stelle zu landen. Der Pilot kann allerdings jeder Zeit die Steuerung übernehmen. Er wird feststellen, dass die Drohne, besonders bei starkem Wind, viel leichter abdriftet. Da sie nun einzig auf den Beschleunigungssensor für die Stabilisierung angewiesen

[5] https://www.admin.ch/opc/de/classified-compilation/19920153/index.html
[6] https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/technologien/videoueberwachung/videoueberwachung-mit-drohnen-durch-private/videoueberwachung-mit-drohnen-durch-private.html
[7] Zitat: Bundesgesetz über den Datenschutz
[8] https://www.jammer-shop.com/de/gps-stoesender.html

ist. Dieser nimmt leichte Abdrifts allerdings nur schwer wahr. Allerdings ist ein guter Pilot auf eine solche Situation vorbereitet und kann die Drohne auch ohne GPS manövrieren und hat dies auch schon geübt. Hierzu kann das GPS auch manuell bei der Drohne ausgeschalten werden. Besonders bei Indoor Flügen wird dies oft gemacht, da der GPS Empfang drinnen oft schlecht oder gestört sein kann. Mittels GPS Jamming kann eine Drohne also nicht vom Himmel geholt werden, es kann höchstens das automatische Abfliegen von Wegpunkten unterbunden werden, dem Piloten das Fliegen erschwert werden und gewisse Sicherheitsautomatismen unterbunden werden wie z.B. die Coming Home Funktion bei Signalverlust.

Angriff auf Kompass

Um sich in der Z-Achse zu orientieren besitzen viele Drohnen einen Magnetsensor, welcher das Erdmagnetfeld misst. Dieser Kompass hat zwei grundlegende Aufgaben. Einerseits sorgt er dafür, dass sich die Drohne nicht anfängt zu drehen, andererseits wird er benötigt beim Abfliegen von Wegpunkten. Hier hilft der Kompass die Richtung, in welcher der nächste Wegpunkt liegt, zu ermitteln. Aus meiner eigenen Erfahrung ist dieser Magnetsensor sehr anfällig, ein stahlarmierter Untergrund reicht bereits, aus um diesen zu verwirren. Mit einem starken Magnetfeld könnte nun der Drohne ein falscher magnetischer Norden vorgegaukelt werden und sie würde im Wegpunktmodus in die falsche Richtung fliegen. Dies gilt allerdings nur für den automatischen Modus. Im normalen Freiflugmodus könnte dieser Angriff im besten Falle zu einer leichten Drehung der Drohne führen, da sie sich in der Z-Achse nicht mehr orientieren kann. Allerdings nimmt hier der Beschleunigungssensor immer noch eine relative Änderung war.

Angriff auf Verbindung

WiFi

Wird die Drohne mittels WiFi gesteuert, ist eine Übernahme der Drohne relativ leicht, wie folgendes Video ausdrücklich zeigt[9]. Allerdings ist die Reichweite von WiFi sehr eingeschränkt, weshalb relativ wenige Hersteller besonders von grösseren Drohnen darauf setzten. Auch die Übernahme von Kleinstdrohnen, die mittels Bluetooth gesteuert werden, sollte kein grosses Problem sein.

Telemetrie Link

An der Black Hat Asia 2016 demonstrierte Nils Rodday, wie es möglich ist, den Telemetrielink, welcher auf dem XBee Protokoll basiert, zu übernehmen. Diese Sicherheitslücke ist allerdings inzwischen laut seinen Aussagen geschlossen und betrifft vor allem professionelle Drohnen, welche diesen Link einsetzten[10].

[9] https://www.youtube.com/watch?v=qYL23IGPz30&t=158s
[10] https://www.youtube.com/watch?v=JRVb-xE1zTI&t=1489s

DJI OcuSync

Der grösste Anbieter von Hobby Drohnen ist DJI, diese verwenden ihre selbst entwickelte Verbindung namens OcuSync. Diese operiert auf dem 2.4 und 5.8 Ghz Frequenzband und kann 1080p Videosignal bis zu 7km weit übertragen. Wie genau dies funktioniert ist Geschäftsgeheimnis und wird auch streng behütet. Aktuell kommt keiner der Konkurrenten auf solche Werte. Aktuell haut auch noch niemand dieses Protokoll reverse engineered, darum sind auch noch keine Schwachstellen darüber bekannt.

Angriff auf Remote Controller

Bei vielen Drohnen dient ein Smartphone zur Anzeige der Telemetriedaten, wie auch das Videosignal oder der Remote Controller selbst basiert auf einem Android Betriebssystem. Hat man die Kontrolle über dieses Gerät, wäre es leicht die Drohne zu übernehmen. Entweder in dem man dem User eine gefälschte Applikation unterjubelt, auf die ich Kontrolle habe oder andererseits ist es auch nicht ausgeschlossen, dass die originalen Applikationen Lücken aufweisen, welche vom übernommenen Betriebssystem ausgenutzt werden können. Dies ist aber relativ aufwändig und fordert entweder Zugriff auf das physische Gerät oder deren Internetverbindung, um Schadcode einschläussen zu können. Zudem sind natürlich hier die Betriebssystem Hersteller daran interessiert, solche Lücken nicht entstehen zu lassen resp. zu schliessen. Die Vielzahl and Betriebssystemen und Versionen macht hier einen grossflächigen Angriff sehr schwer.

Angriff auf Steuerungscontroller

Jede Drohne hat einen Mikrocontroller an Board, welcher für die Stabilisierung, Kontrolle der Drohne sowie den Empfang der Steuerungsdaten verantwortlich ist. Hat man Zugriff auf diesen, kann eine Drohne tatsächlich manipuliert und vom Himmel geholt werden. Ohne physischen Zugriff auf diesen ist es aber sehr unwahrscheinlich resp. nicht lohnenswert diesen zu übernehmen.

Drone Detection Platform

Der Drohnenhersteller DJI selbst bietet eine Platform an, welche es ermöglicht, Drohnen aufzuspüren. Diese erlauben es zwar nicht, Kontrolle über die Drohne zu erlangen, da eine forcierte Landung jeweils auch Personen am Boden gefährdet. Sie zeigt dem Benutzer aber die genaue Position der Drohne wie auch des Piloten an, so wie die Kontaktdaten im hinterlegten DJI Account. (Aussage DJI Importeur Schweiz) Offizielle Angaben müssten vom Hersteller angefordert werden und sind nur unter Verschluss zugänglich. Diese ist allerdings nicht frei verkäuflich und wird ausschliesslich an Regierungsorganisationen, so wie Betreiber kritischer Infrastruktur, verkauft[11].

[11] https://www.dji.com/ch/aeroscope

Physische Abwehr

Greifvögel

In verschiedenen Presseartikeln[12] wird immer wieder von Greifvögeln berichtet, die auf Drohnenjagd gehen sollen. Schon seit Tausenden von Jahren, werden z.B. Adler zur Jagd eingesetzt. Allerdings ist das Ganze in der Praxis nicht sehr praktikabel, da nur hungernde Vögel wirklich jagen. Zudem sind die Propeller der Drohne eine Gefahr für die Vögel. Darum hat z.B. die niederländische Polizei ihr Programm wieder eingestellt[13].

Fangnetze

Auch Fangnetze für Drohnen werden immer wieder in den Medien erwähnt[14]. Entweder können sie an einer Drohne montiert oder mittels Wurfgeschoss abgefeuert werden[15]. Das Hauptproblem hier ist die Gefahr für Personen, die sich unter der Drohne befinden und von der herabfallenden Drohne verletzt werden können. Besonders bei Grossveranstaltungen ist eine solche Methode sehr gefährlich.

Fazit

Eine Drohne zu übernehmen ist, wenn dann nur mit sehr hohem Aufwand, möglich und in der Realität nicht sehr praktikabel. Zudem entsteht bei einem kontrollierten Absturz ein hohes Risiko für umliegende Personen. In der Praxis wird sich vermutlich eine Drone Detection Platform durchsetzen, welches es Flughäfen, Gefängnissen oder Energiekraftwerken erlaubt, Drohnen so wie deren Piloten schnell ausfindig zu machen. Ausserdem sind viele der Anfängerdrohnen mit No-Fly Karten ausgestattet und erlauben es gar nicht in solche Bereiche einzudringen.

[12] https://www.tagesanzeiger.ch/sonntagszeitung/in-genf-gehen-adler-auf-drohnenjagd/story/27631914
[13] https://www.nzz.ch/panorama/niederlaendische-polizei-entlaesst-ihre-anti-drohnen-greifvoegel-ld.1339000
[14] https://www.stern.de/panorama/weltgeschehen/jagd-auf-drohnen–japans-polizei-will-unbemannte-flugobjekte-mit-netzen-fangen-6603656.html
[15] https://www.koller.engineering/net-gun/