# How to hack a drone

## Wie funktioniert eine Drohne

Umgangssprachlich wird oft der Begriff Drohne verwendet, damit ist in der allermeisten Fällen von Multikoptern die rede. //TODO Beschreiben automatischer Modus/ Wegpunktmodus

## 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)[https://www.admin.ch/opc/de/classified-compilation/19940351/index.html] Abschnitt 7: Unbemannte Luftfahrzeuge bis 30 kg Gewicht geregelt. Dabei gelten folgende Regeln:

1 Wer ein Modellluftfahrzeug mit einem Gewicht bis 30 kg betreibt, muss stets direkten Augenkontakt zum Luftfahrzeug halten und jederzeit die Steuerung gewährleisten können 2 Der Betrieb von Modelluftfahrzeugen mit einem Gewicht zwischen 0,5 und 30 kg ist untersagt: a. in einem Abstand von weniger als 5 km von den Pisten eines zivilen oder militärischen Flugplatzes; b.3 in aktiven CTR, sofern dabei eine Höhe von 150 m über Grund überstiegen wird; c.4 im Umkreis von weniger als 100 Metern um Menschenansammlungen im Freien, es sei denn, es handle sich um öffentliche Flugveranstaltungen nach Artikel 4. Zitat: https://www.admin.ch/opc/de/classified-compilation/19940351/index.html

Das BAZL selbst spricht von einer Menschenansammlung ab 24 Personen.

Zusätzlich wird in Artickel 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, diese findet man üblicherweise auf deren Webseite. Eine Übersicht darüber gibt es leider nicht. Ein Beispiel dafür ist die Gemeinde Augst (https://www.augustaraurica.ch/fileadmin/user\_upload/1\_Besuchen/1\_Allgemeine\_Informationen/Regeln\_fur\_den\_Betrieb\_von\_Drohnen\_und\_Flugmodellen\_Gemeinde\_Augst.pdf)

Ab Januar 2021 wird die Schweiz die Drohnenregelung der EASA (European Union Aviation Safety Agency) einführen (https://www.bazl.admin.ch/bazl/de/home/gutzuwissen/drohnen-und-flugmodelle/Europaeische\_Drohnenregulierung\_uebernommen.html) 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 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 Coronakriese auf Januar 2021 verschoben.

### Rechtliche Grundlagen zur Privatsphäre, Kameras an Drohnen

Sind auf den Aufnahmen bestimmte oder bestimmbare Personen ersichtlich gilt die Datenschutzverordnung (https://www.admin.ch/opc/de/classified-compilation/19920153/index.html)

Unter folgendem Link hat der Eidgenösische Datenschutz- und Öffentlichkeitsbeauftragte die Regeln zusammen gefasst (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/technologien/videoueberwachung/videoueberwachung-mit-drohnen-durch-private/videoueberwachung-mit-drohnen-durch-private.html)

Es gelten folgende Regeln:

## Angrifsszenarien

### Angriff auf GPS

Mittels eines GPS Jammers kann der Drohne die Verbundung zu GPS Satelliten erschwert werden. Diese Geräte sind in der Schweiz offiziel verboten, sind aber trotzdem natürlich im Internet bestellbar (https://www.jammer-shop.com/de/gps-stoesender.html). 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 Beschleunigungssensnor für die Stabilisierung angewiesen 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 manöfrieren 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, anderererseits 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-Achste nicht mehr otientieren 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 eindrücklich zeigt (https://www.youtube.com/watch?v=qYL23IGPz30&t=158s) 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 vorallem Professionelle Drohnen welche diesen Link einsetzten. https://www.youtube.com/watch?v=JRVb-xE1zTI&t=1489s

#### DJI OcuSync

Der grösste Anbieter von Hobby Drohnen ist DJI, diese verwenden ihren selbst entwickelte verbindung OcuSync. Aktuell sind aber dazu keine Sicherheitslücken öffentlich bekannt.

### Angriff auf Remote controller

Bei vielen Drohnen dient ein Smartphone zur Anzeige der Telemetriedaten wie auch dem Videosignal oder der Remote Controller selbst basiert auf einem Android Betriebssystem. Hat man die Kontrolle über dieses Gerät, wäre es ein leichtes die Drohne zu übernehmen. Entweder in dem man dem User eine gefälschte Applikation unterjubelt, auf die ich Kontrolle habe oder andererseit 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 einschläusen 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 Grossflächichen Angriff sehr schwer.

### Angriff auf Steuerungs controller

Jede Drohne hat einen Mikrocontroller an Board, welcher für die Stabilisierung Kontrolle der Drohne sowie Empfang der Steuerungsdaten verantwortlich ist. Hat man Zugriff auf diesen, kann eine Drohne tatsächlich manipiliert und vom Himmel geholt werden. Das dieser Controller keine Schwachstellen hat, kann natürlich nicht ausgeschlossen 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 nehemen, da eine forcierte Landung jeweils auch Personen am Boden gefärdert. Sie zeigt dem Benuzer 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. https://www.dji.com/ch/aeroscope

### Physische Abwehr

#### Greifvögel

In verschiedenen Presseartikeln (https://www.tagesanzeiger.ch/sonntagszeitung/in-genf-gehen-adler-auf-drohnenjagd/story/27631914) wird immer wider von Greifvögeln berichtet, die auf Drohnenjagt gehen sollen. Schon seid 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 wider eingestellt (https://www.nzz.ch/panorama/niederlaendische-polizei-entlaesst-ihre-anti-drohnen-greifvoegel-ld.1339000)

#### Fangnetze

Auch Fangnetzte für Drohnen werden immer wider in den Medien erwähnt (https://www.stern.de/panorama/weltgeschehen/jagd-auf-drohnen–japans-polizei-will-unbemannte-flugobjekte-mit-netzen-fangen-6603656.html) Entweder an einer Drohne montiert oder mittels Wurfgeschoss abgefäuert werden können. (https://www.koller.engineering/net-gun/) 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 einnem konntrollierten 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 auffindig zu machen. Ausserdem sind viele der Anfängerdrohnen mit No-Fly Karten ausgestattet und erlauben es gar nicht in solche Bereiche einzudringen.