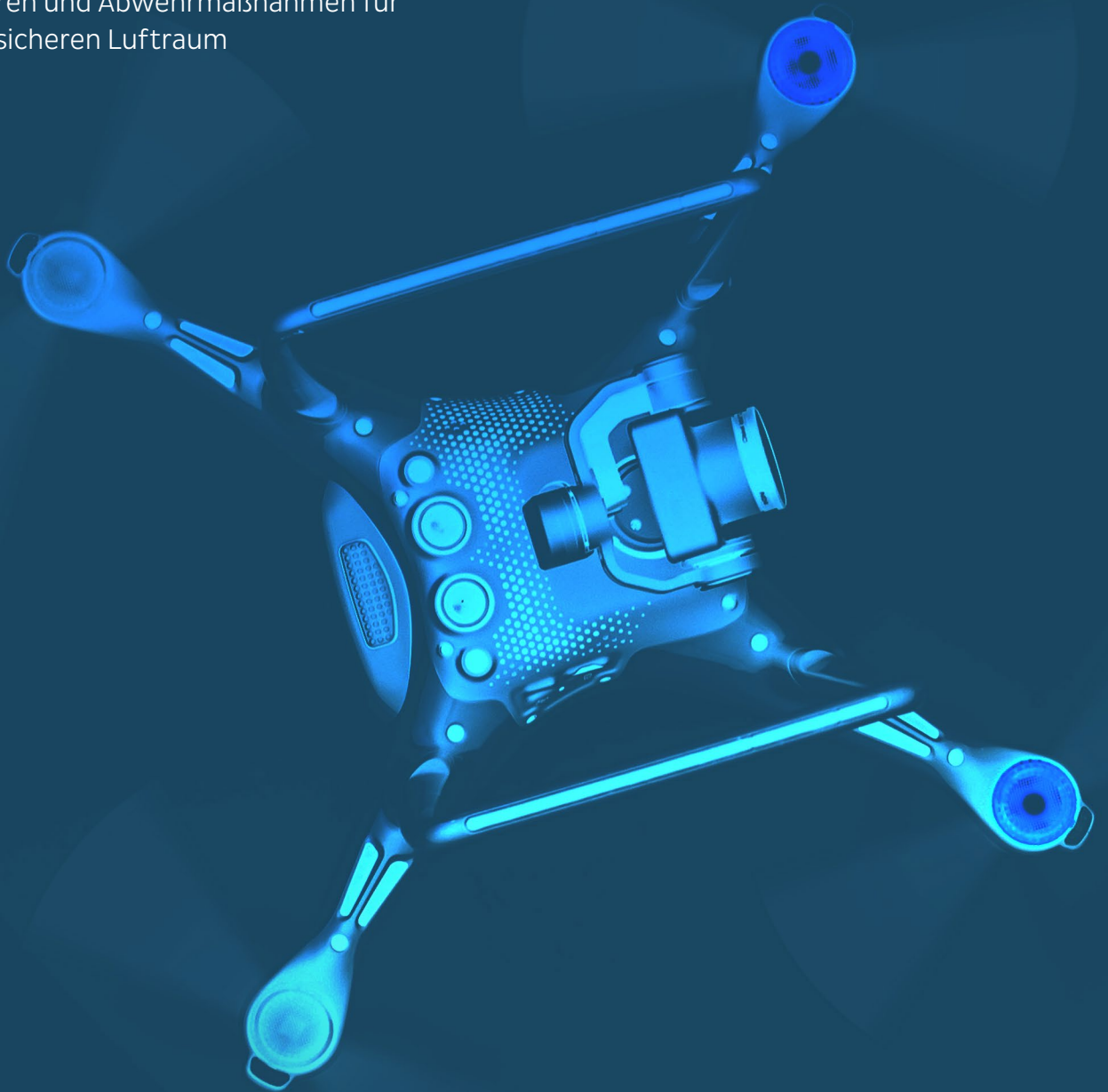


# Gefahren durch Drohnen detektieren und abwehren

Sensoren und Abwehrmaßnahmen für  
einen sicheren Luftraum



# Wie Drohnen detektiert und Bedrohungen entschärft werden

Der Drohnenmarkt entwickelt sich rasant – und ebenso der Markt für Luftraumsicherheit. Als Pionier und Experte auf diesem Gebiet helfen wir unseren Kunden weltweit, die aktuellen Entwicklungen einzuordnen und zu bewerten. Dabei beginnen wir immer mit der Erklärung wichtiger Begriffe.

## Arten der Drohrendetektionstechnologie

### Aktive Detektion: Strahlen aussenden

#### Radar

Ein Gerät, das elektromagnetische Wellen verwendet, um Objekte zu erkennen. Ein Radar sendet ein Signal aus und empfängt und analysiert die reflektierten Echos. Diese Informationen verwendet es, um Richtung und Entfernung des Objekts zu ermitteln. Da ein Radar Strahlen aussendet, braucht man für den Betrieb eine Genehmigung – in Deutschland von der Bundesnetzagentur.

### Passive Detektion: Signale empfangen

#### Radiofrequenz-Sensor

Dieser Sensor hat Antennen, um Radiofrequenzen und -wellen zu empfangen und zu identifizieren.

#### Audio-Sensor

Ein Audio-Sensor, auch Mikrophon genannt, detektiert und analysiert Töne.

#### Optischer Sensor

Ein anderes Wort für Kamera, also ein Gerät, das Lichtveränderungen erkennt und Bilder oder Videos aufzeichnet.



**Das Dedrone-System** sammelt Informationen verschiedener Sensoren, analysiert sie und löst eine Reaktion aus. Unsere Software ist „Sensoragnostisch“, das bedeutet, dass verschiedene Detektionstechnologien mit ihr verbunden werden können. [DroneTracker](#), Dedrones Machine-Learning Software führt die Daten aller Sensoren zusammen, um umgehend entscheiden zu können, ob eine Drohne eine Bedrohung darstellt oder nicht.

# Passive Gegenmaßnahmen

Sogenannte passive Maßnahmen schützen Einrichtungen, ohne in den Luftraum bzw. den Drohnenflug einzugreifen – zum Beispiel, indem Menschen in Sicherheit gebracht oder (Zellen-)Türen und Tore verschlossen werden, man die Sicht auf sensible Bereiche versperrt, Teile der IT-Infrastruktur abschaltet oder das Gelände nach abgeworfenen Gegenständen durchsucht.

- **Alarm auslösen**

Alarmer oder Nachrichten, die an Computer, Mobiltelefone oder andere Geräte geschickt werden, informieren das Sicherheitspersonal sofort über das Heranfliegen einer Drohne.

- **Wi-Fi-Netzwerke sichern**

Dort, wo Daten-Hacking befürchtet wird, wird das Wi-Fi-Netzwerk während der Anwesenheit der Drohne vorübergehend abgeschaltet, um Hacker-Angriffe zu verhindern.

- **Personen und sensible Objekte aus der Sichtlinie nehmen**

Personen können zum Beispiel unter eine Überdachung, von der Terrasse ins Haus oder weg vom Fenster in einen anderen Raum gebracht werden.

- **Sicht versperren**

Bewegliche Dächer werden geschlossen, Rollläden heruntergelassen oder zu schützende Objekte wie Prototypen rechtzeitig verhüllt.

- **Nebelbomben, Stroboskope und andere Ablenkungen**

Diese Geräte unterbrechen die Sichtlinie zum Ziel des Drohnenpiloten – besonders sinnvoll ist dies bei Spionage.

## Vorteile

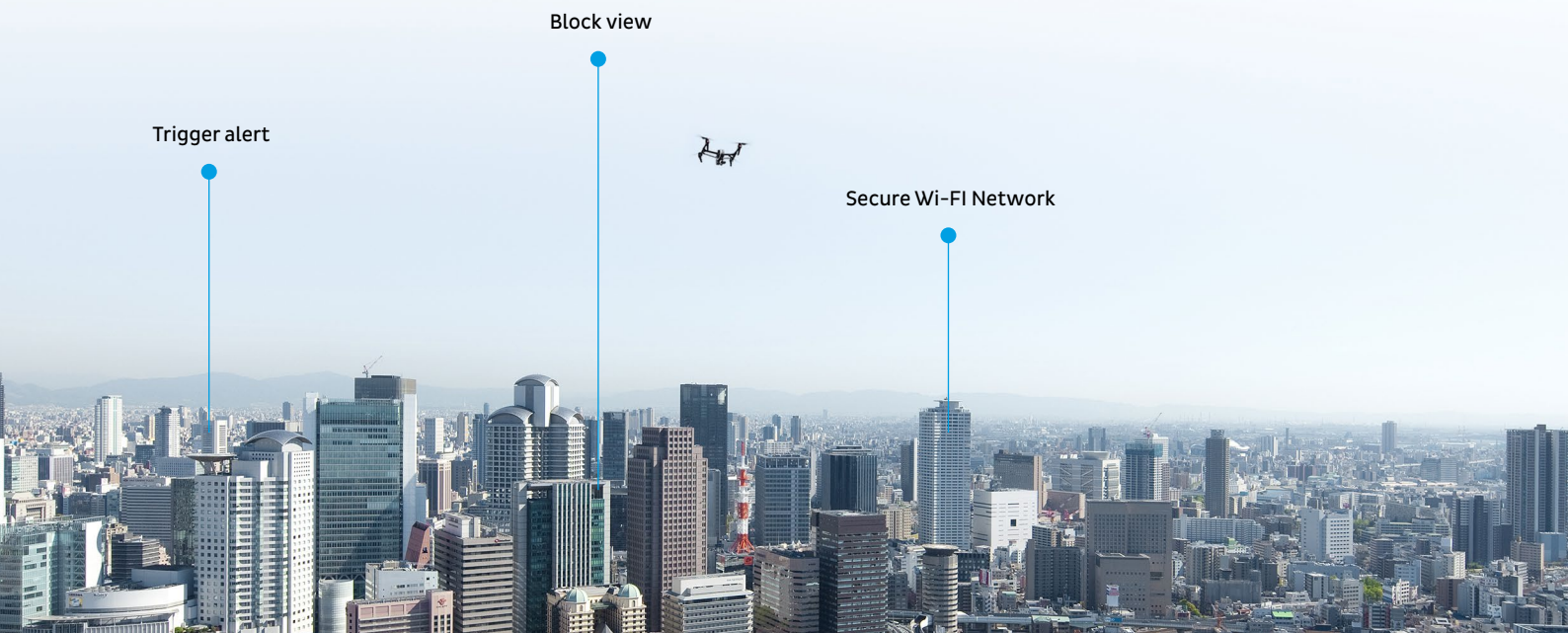
- Effektiv
- Nicht genehmigungspflichtig
- Detailliert kontrollierbar

## Nachteile

- Drohnenflug wird nicht gestoppt

## Schützen Sie Ihre Einrichtung

Mit Drohnen können selbst eingezäunte Gefängnisse leicht ausgespäht werden. Die Analyse- und Berichtsfunktion der [DroneTracker-Software](#) ermöglicht Sicherheitsteams, Muster in den Drohnenaktivitäten zu erkennen und die Sicherheitsvorkehrungen anzupassen.



# Aktive Gegenmaßnahmen

Eine Drohne aktiv abzuwehren bedeutet, sie zum Landen, Anhalten oder Umkehren zu bewegen oder sie sogar zu zerstören. Viele aktive Maßnahmen sind allerdings nicht erlaubt, genehmigungspflichtig oder Regierungsorganisationen vorbehalten.

- **Jamming:** Ein Jammer sendet ein Störsignal, das die Funkverbindung zwischen Fernsteuerung und Drohne übersteuert und unterbricht. Das Signal des Jammers stört gezielt die Kommunikationskanäle der Drohne und behindert die Navigation. In den meisten Fällen führt das dazu, dass die Drohne stehen bleibt und zur Landung gezwungen wird. Das Jamming gilt als effektivste Abwehrmaßnahme.
- **Spoofing:** Beim Spoofing werden der Drohne falsche GPS-Datenpakete gesendet, um sie zu verwirren. Für das Fluggerät sieht es so aus als würden die Signale vom Satelliten kommen, was dazu führt, dass die Drohne denkt, sie sei an einer anderen Position. Mittels Spoofing ist es möglich die Drohne von ihrer eigentlichen Route abzubringen.
- **Hacking:** Ähnlich wie beim Spoofing werden der Drohne beim Hacking falsche Datenpakete übermittelt. Das Fluggerät wird verwirrt und kommt von seiner Bahn ab. In wenigen Fällen ist es, je nach Drohnenmodell, sogar möglich die Steuerung zu übernehmen.
- **Fangnetz:** Ein Netz, das mit einer speziellen Kanone auf eine Drohne geschossen wird, um diese zu stoppen.
- **Fangdrohne:** Eine Drohne wird mit einem Netz ausgestattet und versucht die angreifende Drohne einzufangen und den Flug zu beenden.

## Zerstörer

- **Laser:** Ein optisches Gerät, das einen starken Strahl aus elektromagnetischen Wellen auf die Drohne richtet. Abhängig von der Leistung des Lasers kann er die Hardware oder die Kamera verbrennen oder blenden.
- **Elektromagnetischer Impuls (EMP):** Ein Generator sendet einen Energieimpuls aus, der, wenn er stark genug ist, schwach abgeschirmte Elektronik beschädigen kann.
- **Hochenergie-Mikrowellen:** Mikrowellen werden von einer Antenne erzeugt – wie in Mikrowellengeräten, die Speisen erhitzen. Wenn ein Maiskorn in eine Mikrowelle gelegt wird, explodiert es und wird zu Popcorn. Wenn eine Hochenergie-Mikrowelle auf eine Drohne zielt, wird diese zerstört.

## DroneDefender

- Störung der Fernsteuerung
- Störung des GPS-Empfängers
- Tragbar
- Nicht-kinetisch
- Verringert das Risiko von Kollateralschäden

Weitere Informationen zum DroneDefender finden Sie unter [www.dedrone.com](http://www.dedrone.com).



**Dedrone** ermöglicht eine Erweiterung seines Drohnenabwehrsystems durch die Integrierung von Sensoren wie PTZ-Kameras und Radarsystemen. Für Organisationen, die eine behördliche Genehmigung haben, bietet Dedrone seine nicht-kinetische Lösung zur Drohnenabwehr an. Der **DroneDefender** ist ein tragbarer, RF-basierter Jammer, der die Funkverbindung zwischen der Fernsteuerung und der Drohne unterbricht und den Flug beendet, ohne die Umgebung zu gefährden oder Kollateralschäden zu riskieren.

**Germany**

Miramstraße 87  
34123 Kassel

**Headquarter**

220 Sansome St. 6th Floor,  
San Francisco, CA 94104

**Washington, D.C.**

45662 Terminal Dr.  
Sterling, VA 20166

**United Kingdom**

Building 1, Chalfont Park,  
Gerrards Cross SL9 0BG,  
Buckinghamshire

Weitere Informationen finden Sie unter [www.dedrone.com](http://www.dedrone.com)

© Dedrone 7/2020, V2