

# Mehrschichtige Drohnenabwehr

## ► Technologischer Weitblick für den Luftraum

Mit der zunehmenden Verbreitung ziviler und kommerzieller Drohnen wächst auch das Bedrohungspotenzial, insbesondere für kritische Infrastrukturen, Industrieanlagen und militärische Einrichtungen.

**D**rohnen können nicht nur zur Spionage oder Sabotage eingesetzt werden, sondern auch gezielt Sicherheitslücken ausnutzen, indem sie physische oder digitale Schutzmechanismen umgehen. Vor diesem Hintergrund gewinnt ein ganzheitliches Drohnenabwehrkonzept an Bedeutung, insbesondere auf Basis eines mehrschichtigen Sicherheitsansatzes und der intelligenten Integration von Sensoren und Effektoren in ein zentrales Perimeter-Management-System.

### Bedrohungen aus der Luft: Drohnen als reale Gefahr

Moderne Drohnen sind klein, wendig, kaum hörbar und lassen sich mit wenig Aufwand manipulieren. Sie überfliegen Absperrungen, erkennen Schwachstellen und agieren teilweise autonom. Das macht sie zu einem besonders schwer fassbaren Risiko, sei es für Großveranstaltungen, Regierungsgebäude, Energieversorger oder Forschungseinrichtungen. Eine isolierte Maßnahme reicht hier

nicht aus: Erforderlich ist ein abgestuftes, dynamisches und ganzheitlich vernetztes Detektions- und Abwehrsystem.

### Detektion, Klassifikation, Reaktion

Ein effektives Drohnenschutzsystem folgt einem mehrschichtigen Prinzip, bei dem verschiedene Sensoren, Analyseverfahren und Abwehrmaßnahmen nahtlos ineinandergreifen. Ziel ist es, Bedrohungen im Luftraum frühzeitig zu erkennen, präzise zu bewerten und gezielt abzuwehren.

Bereits in der ersten Ebene erfolgt die Detektion durch unterschiedliche Sensoren wie Radar oder Radiofrequenzscanner (cRF). Diese erfassen verdächtigen Flugverkehr und liefern erste Datenpunkte zu Position, Geschwindigkeit und Modell. Die nächste Schicht dient der Klassifikation: KI-gestützte Kameras und Analysetools werten Flugverhalten, Frequenzmuster sowie visuelle Merkmale aus. Dadurch kann unterschieden werden, ob es sich um harmlose Hobbydrohnen oder potenzi-

ell bedrohliche UAVs handelt („Freund oder Feind“-Erkennung).

Herzstück des Systems ist die KI-Fusion-Engine, welche die Daten aus sämtlichen Sensorquellen intelligent zusammenführt, gewichtet und interpretiert. Durch diese Fusion entsteht ein umfassendes Lagebild, das nicht nur einzelne Signale isoliert betrachtet, sondern Zusammenhänge erkennt und daraus konkrete Handlungsempfehlungen ableitet. Dadurch wird der Bediener entlastet und kann in kritischen Situationen schneller und fundierter reagieren.

Auf dieser Grundlage folgt in der dritten Ebene die Reaktion: Je nach Bedrohungslage werden geeignete Effektoren aktiviert: von der gezielten Funkstörung (Jamming) über physische Abwehrmaßnahmen (z.B. mit Netzen) bis hin zur kontrollierten Übernahme und sicheren Landung unkooperativer Drohnen per Cybertechnologie. Auch hier koordiniert die Fusion-Engine das Zusammenspiel aller Komponenten und stellt sicher, dass Maßnahmen effizient und situationsgerecht erfolgen.

So entsteht ein intelligentes, adaptives Sicherheitsnetz im Luftraum, das präventiv, reaktiv und kontinuierlich auf

unterschiedlichste Bedrohungsszenarien reagieren kann, um den Anwender durch automatisierte Analyse und Entscheidungsunterstützung bestmöglich zu unterstützen.

### Dome Security: Luft- und Bodensicherheit intelligent vernetzt

Die reine Luftraumüberwachung ist jedoch nur ein Teil eines umfassenden Sicherheitskonzepts. Erst durch die Einbindung weiterer Schutzmaßnahmen wie Videoüberwachung, Zutrittskontrollsysteme, Zaundetektion oder Robotiksicherheitslösungen, lässt sich ein vollständiger Schutzbereich realisieren. Diese verschiedenen Systeme agieren nicht isoliert, sondern werden in einer zentralen Softwareplattform, dem Perimeter-Management-System, intelligent miteinander verknüpft. Sie erfasst, priorisiert und visualisiert Bedrohungslagen in Echtzeit, steuert automatisierte Reaktionen und unterstützt Sicherheitspersonal bei der Lagebewertung. So entsteht eine digitale „Kuppel“ über zu schützenden Bereiche: von der Luft bis zum Boden, vom Außenbereich bis ins Herz der Infrastruktur.

### Fazit: Schutz durch Vernetzung und Schichtung

Drohnensicherheit lässt sich nicht mit einem einzelnen Tool gewährleisten. Der Schlüssel liegt in der Mehrschichtigkeit – in der Kombination verschiedener Sensor- und Abwehrtechnologien, die durch eine intelligente Plattform koordiniert und gesteuert werden. Ein modernes Perimeter-Management-System verbindet diese Ebenen zu einem adaptiven, quasi lückenlosen Schutzschirm, der sowohl präventiv als auch reaktiv funktioniert. Gerade in Zeiten wachsender technologischer Risiken ist diese vernetzte Sicherheitsarchitektur nicht nur sinnvoll, sondern zwingend notwendig.

[www.securiton.de](http://www.securiton.de)

◀  
Lückenlose Sicherheit:  
Das Dome-Security-Konzept  
Foto: Securiton GmbH