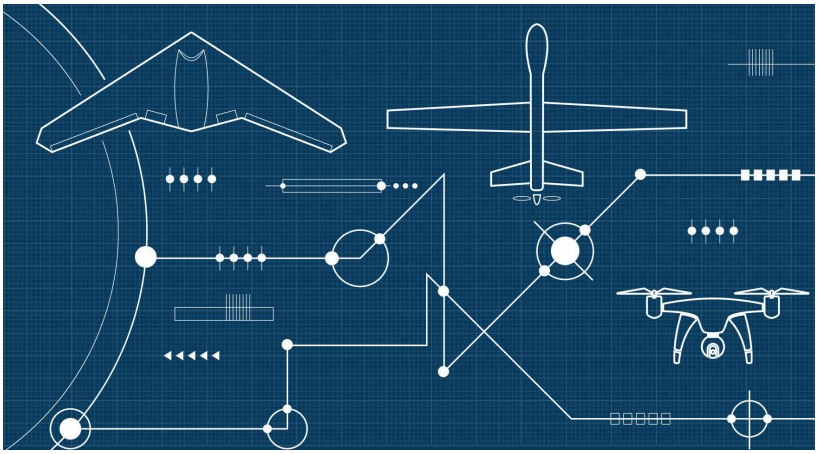

Deutsche Fassung des Kapitels 20 (ab Seite 350) aus dem Fachbuch:

A Comprehensive Approach to Countering Unmanned Aircraft Systems

Herausgeber:
Joint Air Power
Competence Center
47546 Kalkar | www.japcc.org

Cloudbasierte Steuerung und Kontrolle für Sicherheits- und Drohnenabwehranwendungen

Georg Schweizer, Senior Consultant Mobiler Objektschutz, Securiton Deutschland

Kleine Drohnensysteme für den privaten und gewerblichen Gebrauch bestehen aus vielen Hightech-Komponenten und ermöglichen dem Menschen viele neue nützliche Anwendungen. Drohnen sind jedoch auch ideale Hilfsmittel für Kriminelle und Terroristen und erweitern deren Möglichkeiten erheblich. Eine effektive Abwehr von Drohnen, die mit bösartigen Absichten zum Einsatz kommen, ist dementsprechend auch nur mit Hightech-Systemen möglich.

Drohnen sind heute überall in großer Anzahl verfügbar und werden immer leistungsfähiger. Die Möglichkeiten und damit die Häufigkeit, mit Hilfe von Drohnen zu belästigen, zu gefährden und kriminelle oder terroristische Taten zu begehen, nehmen damit laufend zu.

Einerseits erlauben es Drohnen einem Täter schnell und unerkannt zu handeln und damit sein Risiko zu minimieren. Andererseits ist es für das Opfer nicht leicht, eine Drohne zu erkennen und deren Einsatzabsichten sofort zu beurteilen. Ein überraschendes Erscheinen einer Drohne in der Nähe von kritischen Infrastrukturen oder in der Nähe schützenswerter Personen ist grundsätzlich immer als ein bösartiger Drohneneinsatz zu bewerten.

Wie kann man sich vor solchen Überraschungen schützen? Gibt es dafür Abwehrmöglichkeiten, die in der Beschaffung etwa gleich viel kosten wie Drohnensysteme sowie schnell und einfach in jedem Anwendungsumfeld eingesetzt werden können?

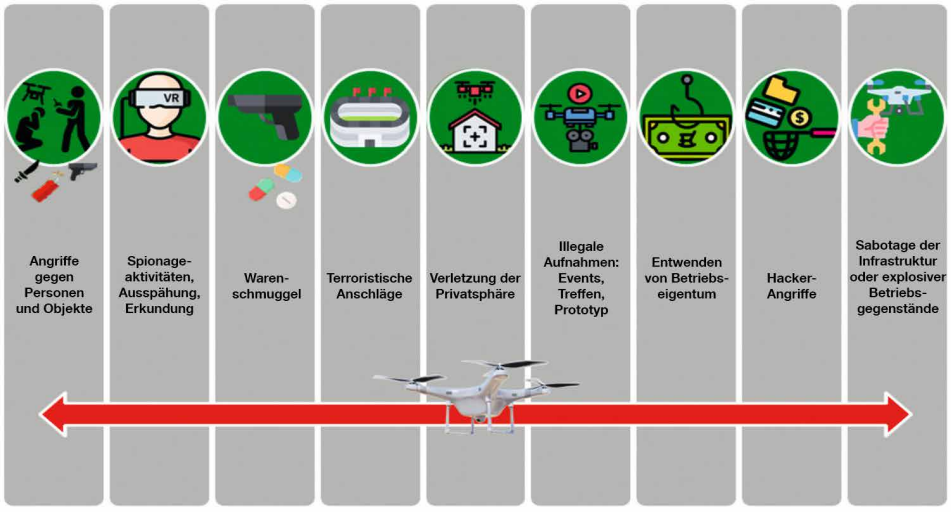

Abbildung: Die üblichen Tatbestände mittels Drohneneinsatz

Traditionelle Schutzsysteme

Historisch wurden zum Schutz von Liegenschaften mit wertvollen Gütern und zum Schutz wichtiger Personen Burgen und Festungen gebaut (Structural measures) und Wachen aufgestellt (Organisational measures). Mussten wichtige Personen das Schutzwerk verlassen oder wertvolle Güter transportiert werden, so wurden sie von verstärkten Wachen begleitet.

Heute werden zum Schutz wichtiger Infrastrukturen neben Zäunen, Mauern und Panzerungen auch technische Geräte wie Brandmeldeanlagen, Einbruchmeldeanlagen, Videosicherheitssysteme etc. (Technical measures) als Hilfsmittel für Eingangskontrollen, Wachmänner und Einsatzkräfte eingesetzt. Teil der organisatorischen Maßnahmen sind dabei auch Risikoanalysen sowie Maßnahmen und Einsatzpläne beim Auftreten einer Gefahr zur Abwehr und zur Schadensbegrenzung.

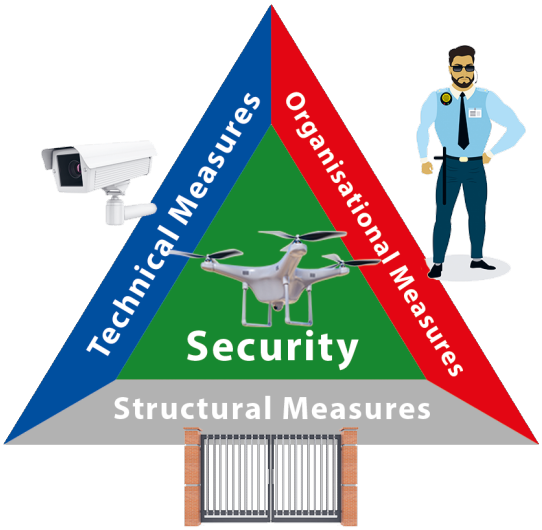

Abbildung: Das Sicherheitsdreieck

Die beste Sicherheit in Bezug auf Risiken ist dann gegeben, wenn die drei verschiedenen Gruppen von Maßnahmen optimal aufeinander abgestimmt sind.

Zum Schutz gegen einen Drohneneinsatz kann man Personen und wichtige Gegenstände in ein Gebäude (Schutzraum) bringen und sämtliche Eingänge und Fenster schließen. Dies ist allerdings ein sehr umständliches Verfahren. Im freien Luftraum hingegen sind gegen Drohnen praktisch keine strukturellen Maßnahmen möglich. Ein Schutz gegen Drohnen ist mit organisatorischen Maßnahmen, wie zum Beispiel Wachpersonal für die Luftraumüberwachung, praktisch auch nicht möglich, da Drohnen mit ihrer Größe und Geschwindigkeit, eingesetzt im nahen Luftraum, einem Menschen mit seinen Sinnesorganen und seiner Beweglichkeit weit überlegen sind.

Eine Drohnenabwehr ist somit nur mittels spezieller technischer Maßnahmen, verbunden mit entsprechenden organisatorischen Maßnahmen, machbar. Dabei ist zu beachten, dass Drohnen auch dann eingesetzt werden können, wenn wichtige Personen reisen, wertvolle Güter transportiert werden, sich viele Personen an einem Ort versammeln oder wenn wertvolle oder wichtige Güter vorübergehend im Freien gelagert werden.

Drohnenschutztechnologien

Eine Technologie zum Schutz vor Drohnen soll so schnell und so einfach wie möglich und überall einsetzbar sein. Genauso wie auch eine oder mehrere Drohnen schnell, einfach und überall eingesetzt werden können.

Drohnenerkennung (Sensoren)

Um sich vor Drohneneinsätzen zu schützen, muss ein solcher Einsatz zuerst erkannt werden. Dazu braucht es Sensoren wie:

- **Radio Frequency (RF) Sensor**: Der RF-Sensor ist ein Beyond line of sight Sensor, der Drohnen und Drohnenfernsteuerungen auch in großer Distanz erkennen und aus dem Funkspektrum herausfiltern kann. Also auch dann, wenn die Drohne gar nicht in direkter Sichtweite betrieben wird. Er ist der einzige Sensor, der einen Drohneneinsatz schon in der Vorbereitungsphase erkennen kann, und zwar sobald eine Drohnenfernsteuerung aktiviert wird. Intelligente RF-Sensoren erfassen die Inhalte von Funkübertragungen zu Drohnen. Damit können Drohnenmodell, Batterieladezustand und maximale Traglast der anfliegenden Drohne angezeigt werden. Zur genauen 3D-Zielerfassung von Drohnen muss ein RF-Sensor über mindestens 2 (idealerweise 3) verteilte 3D-RF-Antennen verfügen, um die Ziele (Drohnen und Drohnensteuerung) mittels Triangulation ermitteln zu können. Ein einzelner RF-Sensor kann eine Drohne bis auf mehrere Kilometer Distanz erkennen.

- **Akustik Sensor**: Ein Akustiksensor, ein Beyond line of sight Sensor, erkennt das Geräusch von Drohnen-Rotoren, ist jedoch wegen möglichem ähnlichem Umgebungslärm nur für kurze Distanzen geeignet.

- **Radarsensor**: Ein Radarsensor ist ein In line of side Sensor, der Drohnen in großer Höhe über oder vor dem Horizont erkennen und von anderen Flugobjekten wie Vögel unterscheiden kann. Ein Radar mit 3D-Eigenschaften ermittelt nicht nur die Richtung zum Drohnenziel, sondern auch noch seine Flughöhe und Geschwindigkeit. Spezielle Radare für Drohnensensoren erkennen Drohnen auf eine Distanz von mehreren Kilometern. Abhängig vom Radarmodell und vom Einsatzort benötigen Radarsensoren oftmals Einsatzbewilligungen von Behörden.

- **Videosensor**: Eine Videokamera (Tageslicht- oder Infrarotkamera) ist ein In line of side Sensor und kann eine Drohne mittels eingebauter Bildverarbeitung (Videosensorik) selbstständig erkennen, vorausgesetzt, die Drohne fliegt der Videokamera ins Bild

oder die Drohne soll aus einer vorgegebenen Anflugrichtung erkannt werden. Spezielle Kamerasysteme mit intelligenter Videosensorik erreichen Blickwinkel bis 360°. Eine bewegliche Kamera auf einem Pan-Tilt-Zoom-Kopf ist für eine 360°-Drohnenerkennung meistens auf eine Zieleinweisung durch einen RF-Sensor oder einen Radarsensor angewiesen. Hat eine PTZ-Videokamera eine Drohne jedoch einmal auf dem Schirm, so kann sie der Drohne mittels eingebauter Videosensorik selbstständig folgen und damit auch live die Bilder der Drohne, ihrer Ladung und ihres Verhaltens übermitteln. Eine PTZ-Hochleistungskamera mit KI-Videosensor kann eine Drohne auf eine Distanz von wenigen Kilometern unidirektional noch erkennbar abbilden und verfolgen.

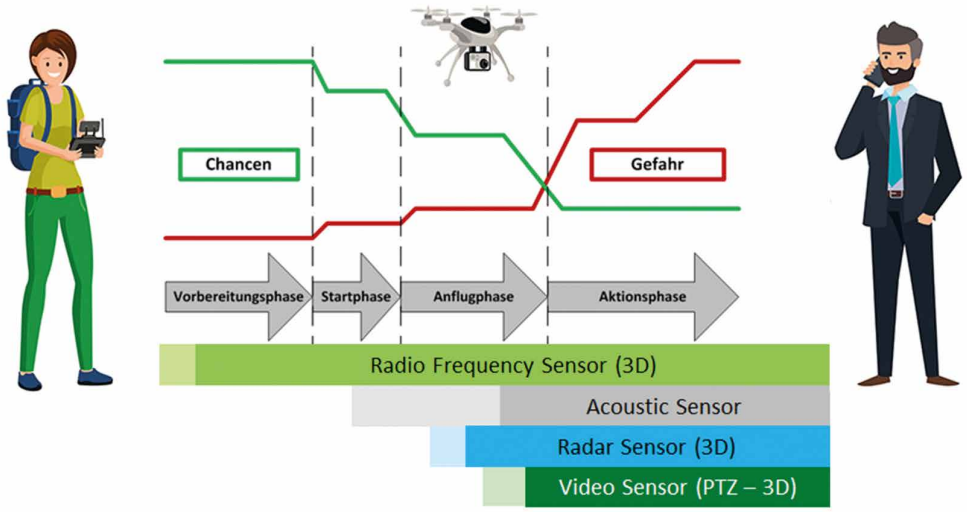

Abbildung: Die Chancen und Risiken einer Drohnenerkennung

- **Identifikationssensor**: Ein Identifikationssender erkennt die Remote-Identifikation, die von einer Drohne ausgesendet wird. Unter dem Begriff „Remote Identification (RID)“ versteht man eine Technik, die die Identifizierung einer Drohne im Betrieb (im Flug) aus der Ferne ermöglicht. Man kann sich das Ganze vereinfacht wie ein Kennzeichen eines PKWs vorstellen. Mit dem Unterschied, dass das Kennzeichen auch dann lesbar ist, wenn die Drohne vielleicht gar nicht in direkter Sichtweite betrieben wird. Neben der weltweit einmaligen Identifikation ist vorgesehen, dass Drohnen auch die aktuelle Position, die Höhe, die Geschwindigkeit und die Flugrichtung laufend aussenden. Getrieben von der EASA (European Union Aviation Safety Agency) sollen Drohnen mit CE-Klasse C1 bis C3 ab dem 01.01.2021 mit Remote Identification ausgerüstet werden [1]. Ab dem 31.12.2022 soll Remote Identification für jede Drohne zum Pflichtbestandteil werden und auch ältere Drohnensysteme damit ausgerüstet sein. Müssen Drohnen dann noch staatlich registriert werden, so kann man über die Identifikation den Besitzer der Drohne erkennbar machen. Der Empfang solcher Drohnenidentifikationssignale wird zukünftig auch mit Smartphones möglich sein. Damit kann jede Privatperson mit der entsprechenden App den Drohnenverkehr in seiner unmittelbaren Nähe verfolgen.

Das ergibt nicht nur für die Luftraumüberwachung, sondern auch für die Drohnenabwehr einen deutlichen Vorteil. Nun müssen alle Drohnen während dem Flug Funksignale aussenden und sind damit für RF-Sensoren dauernd erkennbar, auch wenn sie in vorprogrammierten Flugbahnen (mit Auto Pilot) fliegen. Kommt nun noch ein Identifikationssender hinzu, kann man sofort weitere Informationen über die Drohne gewinnen. Dabei sind Drohnen ohne Identifikation von denen mit Identifikation zu unterscheiden und besonders zu beachten.

Selbst heutige Drohnen ohne RID, die autonom arbeiten oder vorprogrammiert sind, senden normalerweise immer noch Funksignale zurück an die Drohnensteuerung und sind damit für RF-Sensoren erkennbar. Dies gilt ganz besonders, wenn von mitfliegenden Kameras Videosignale an die Bodenstation übermittelt werden. Da schon heute nahezu alle Drohnensteuerungen und Drohnen Funksignale aussenden, sollte die HF-Sensorik für die Erkennung von kleinen Drohnensystemen immer als Primärsensor eingesetzt werden.

Ein einfacher leistungsfähiger RF-Drohnen-Sensor ist schon heute für eine angemessene Investition auf dem Markt erhältlich.

Sollte eine Drohne komplett autonom ohne permanenten Einsatz von Command- and Control-Technik und damit ohne Abgabe von Funksignalen und zukünftig ohne vorgeschriebene Identifikation eingesetzt werden, so ist diese Drohne wie ein Flugobjekt ohne berechenbare Flugbahn zu betrachten. Dafür sind dann zusätzlich andere Sensoren wie ein Radarsensor oder ein Akustiksensor verbunden mit einem Videosensor einzusetzen. In der Regel sollte immer mehr als ein Sensor für eine zuverlässige Drohnenerkennung verwendet werden.

Drohnenabwehr (Aktoren)
Drohnen in der Luft bekämpfen zu müssen ist buchstäblich die zivile Variante der militärischen Luftverteidigungsmission. Obwohl die zivilen Möglichkeiten begrenzt sind, stehen verschiedene Möglichkeiten zur Verfügung, die nachfolgend aufgeführt sind:

- **Funkstörung (Jamming)**: Da heute nahezu alle Drohnensteuerungen und Drohnen Funksignale aussenden, ist die Funkstörung das einfachste und beste Mittel gegen kleine Drohnen. Funkstörung, welche Frequenzen betrifft, die nicht für den privaten Gebrauch freigegeben sind, ist nur staatlichen Organisationen mit Sicherheitsaufgaben vorbehalten. Funkstörung beeinflusst die näher rückende Drohne an ihrer Kommunikation mit der Drohnensteuerung oder an ihrer Positionierung über GPS, um ihren Einsatz abzubrechen. Eingriffe in öffentliche Frequenzen sind jedoch generell verboten und den Behörden vorbehalten.

  Je nach Gerät können alle Frequenzen, bestimmte Frequenzbänder oder nur einzelne Frequenzen gestört werden. Sind die Anflugrichtung und die Sendefrequenzen einer Drohne bekannt, so kann gezielt gestört werden, ohne andere Funkbenutzer übermäßig zu beeinträchtigen. Zu beachten ist dabei, dass die Drohne bei einem Funkunterbruch durch die Störung die Frequenz zur Kommunikation mit der Drohnensteuerung innerhalb des benutzten Frequenzbandes automatisch anpassen kann. Es wird darum meistens das gesamte Frequenzband gestört, das von anfliegenden Drohnen verwendet wird.

- **Ausschalten der Funkfernsteuerung**: Das Ausschalten der Funkfernsteuerung durch Aufsuchen des Drohnenpiloten ist ein sehr wünschenswertes Mittel, auch um juristisch gegen den Verursacher von unerlaubten Drohneneinsätzen vorzugehen. Allerdings muss dafür der Standort des Piloten bekannt sein und die Zeit muss ausreichen, um mit legitimiertem Abwehrpersonal diesen Ort zu erreichen, solange der Pilot mit der Funkfernsteuerung dort noch anwesend ist.

- **Kontrolle übernehmen**: Die vollständige Übernahme der Drohne durch einen Drohnenpiloten der Sicherheitskräfte ist technisch grundsätzlich möglich, jedoch wegen der Komplexität dieser Abwehrmaßnahme nur mit Spezialgerät machbar und staatlichen Spezialkräften vorbehalten.

- **Abschießen**: Das Abschießen von Drohnen mittels Spezialgewehren und Kanonen mit Schrot- und Netzgeschossen, Laser, Schall, Wärme oder elektromagnetischen Impulsen sind technische Möglichkeiten zur Drohnenabwehr. Wegen der Komplexität dieser Abwehrmaßnahmen ist das nur mit Spezialgerät machbar und staatlichen Spezialkräften vorbehalten. Diese haben dann auch allfällige Kollateralschäden ihrer Einsätze zu verantworten.

- **Abfangen**: Es wurde bereits getestet, Drohnen mit ausgebildeten Greifvögeln abzufangen, allerdings mit unterschiedlichem Erfolg und immer mit dem Risiko einer Verletzung des eingesetzten Tieres. Der effektivere Weg ist wahrscheinlich die Verwendung hochentwickelter Abfangdrohnen, die mit speziellen Sensoren und einem Netz ausgestattet sind, um kleine Drohnen zu erfassen und an einen sicheren Ort zu transportieren. Intercept-Drohnen sind bereits auf dem Markt erhältlich. Aufgrund des geringeren Risikos von Kollateralschäden können speziell lizenzierte Versionen in Zukunft sogar für den privaten und kommerziellen Sektor zugelassen werden.

Viele Faktoren wie Drohnengröße, Drohnenanzahl, Geschwindigkeit, Distanzen, Flugverhalten, Topographie, Umgebungsbeschaffenheit, Wetter und Uhrzeit können die Wirksamkeit von Sensoren und Aktoren bei der Drohnenabwehr sehr stark beeinflussen. Wird bei einem Drohneneinsatz Funk eingesetzt, so ist der Einfluss dieser Faktoren auf den Funkeinsatz am geringsten. Damit ist der Funk auch die größte Schwachstelle eines Drohneneinsatzes, um ihn zu erkennen und dagegen vorzugehen.

Im Gegensatz zur Drohnenerkennung sind für den zivilen und kommerziellen Sektor die Möglichkeiten zur Abwehr von Drohnen sehr beschränkt. Auch hier gilt, dass eine Abwehr einer Belästigung, einer Gefahr oder einer Tat mittels Drohnen nur durch erkennen und anzeigen bei der Polizei begegnet werden kann. Ob die Polizei zukünftig in der Lage sein wird, solchen Ereignissen mit Drohnen effektiv zu begegnen, ist heute Gegenstand neuer Gesetzgebungen und neuer Ausrüstungen für die Polizeikräfte. Die beabsichtigte Implementierung von RID und die Registrierung von Drohnen unterstützen diese Ziele jedenfalls.

Steuerung und Kontrolle
Aus Kostengründen steht für kleine Drohnenabwehrsysteme kein spezielles Personal für den 24/7-Betrieb zur Verfügung. Die Meldung erkannter Bedrohungen sowie die Aktivierung von Gegenmaßnahmen müssen über mobile Geräte wie Mobiltelefone oder Tablets erfolgen,

damit das Personal nicht dauerhaft an einen Ort wie an ein Operation Center gebunden ist. Wenn eine Drohne erkannt wird, so wird der Alarm sofort an ein oder mehrere bestimmte mobile Geräte gesendet und die betroffene(n) Person(en) kann/können dann entscheiden, welche weiteren Maßnahmen ergriffen werden müssen. Eine Mindestkonfiguration eines so kleinen Systems arbeitet mit einer Erfassungsreichweite von bis zu 2 km.

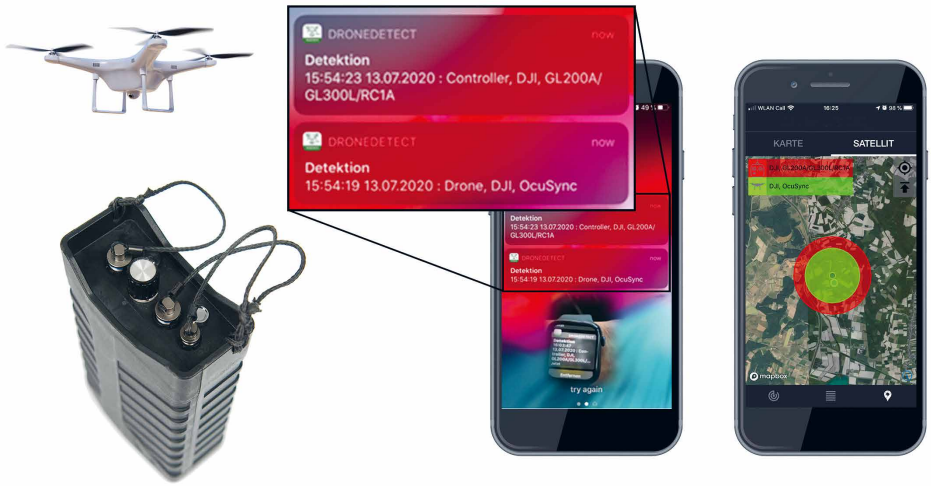

Abbildung: Beispiel eines kleinen tragbaren RF-Sensors (Gewicht < 1kg) und Anzeige einer erkannten Drohnenfernsteuerung und einer Drohne mit Modellangaben, bis auf eine Distanz von 2 km zum RF-Sensor, auf einem Smartphone oder einer Smartwatch an einem beliebigen Standort der sich schützenden Person.

Weiter besteht auch die Möglichkeit, eine Drohnenerkennung und eine Drohnenabwehr an eine mandantenfähige Alarmzentrale anzuschließen und in die dort verfügbaren Steuerungs- und Kontroll-Systeme zu integrieren. Diese Zentralen bearbeiten schon heute die Alarme von Brandmelde- sowie Einbruchmeldeanlagen und Videosicherheitssystemen. Warum also nicht auch Alarme durch unerwünschte oder unerlaubte Drohneneinsätze im Bereich wichtiger Infrastrukturen oder schützenswerter Personen und Objekte. Das dort während 24/7 anwesende Personal kann nach einem Alarm betroffene Personen warnen, Sicherheitskräfte aufbieten oder technisch unterstützende Gegenmaßnahmen auslösen.

Sicherheitsanwendungen und das Internet der Dinge

Das Internet der Dinge (IoT) ist ein Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglichen, physische und virtuelle Gegenstände miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen [2].

Mit Technologien des „Internets der Dinge“ implementierte Funktionen erlauben die Interaktion zwischen Mensch und hierüber vernetzten beliebigen elektronischen Systemen sowie zwischen den Systemen an sich. Sie können darüber hinaus auch den Menschen bei seinen Tätigkeiten unterstützen. Die immer kleineren eingebetteten Computer sollen Menschen unterstützen, und zwar ohne abzulenken oder überhaupt aufzufallen.

Mobile Monitoring (mobile Überwachung) ist in seiner höchsten Stufe das IoT der Sicherheitstechnik. ‚Mobile Monitoring‘ ist ein Sammelbegriff für die zeitbegrenzte Überwachung mittels mobiler technischer Hilfsmittel. ‚Mobile‘ steht dabei für beweglich und ortsveränderlich als auch für Mobilkommunikation. Mobile Monitoring unterstützt Sicherheitsorganisationen und deren Personal bei der Überwachung von Personen und Objekten [3].

Digitale Videotechnik, Audiotechnik, Sensoren, Aktoren, GPS, Funktechnik, Mobilkommunikation, Internet, VPN, Mobile Computing, Cloud-Computing und kleine Akkumulatoren bilden die Grundlagen. Viele dieser Techniken sind auch bei Drohnensystemen im Einsatz.

Natürlich sind (mobile) Überwachungssysteme auch zeitlich unbegrenzt an einem festen Standort zum Schutz von Infrastrukturen und Personen einsetzbar. Die meisten der heute eingesetzten Sicherheitssysteme befinden sich nur an einem Standort, mit dem Zweck, ein Risiko zu vermeiden. Sie sind fest verbaut mit festen Kabelverbindungen für die Energieversorgung und den Datenaustausch. Beispiele solcher Insellösungen sind unter anderem Brandmeldeanlagen, Einbruchmeldeanlagen oder Videosicherheitssysteme mit ihren Sensoren und Aktoren. Diese sind verbunden mit Sirenensystemen und/oder Leitständen mit Bildschirmen, besetzt mit Personal im 24/7 Einsatz, welches bei Alarm die entsprechenden Maßnahmen zur Abwehr und Schadensbegrenzung einleitet.

Drohnensysteme sind andererseits als eine umfassende Anwendung von IoT-Technologien zu betrachten. Gleiches gilt für Mobile Monitoring, die einzige umfassende Alternative zur Abwehr von Drohnen. Dabei müssen beide Systeme im Gleichschritt ihrer technischen Weiterentwicklung bleiben.

Vorteile vernetzter IoT-Sicherheitstechnik

Die Vorteile vernetzter IoT-Sicherheitstechnik speziell für die Drohnenabwehr sind:

- Schnell und überall einsetzbare Sensoren, Aktoren sowie Geräte für Command and Control (C2)

- Temporär oder permanent einsetzbar mit mobilen oder fest verbauten Sensoren, Aktoren sowie Geräten für C2
- Einfach zu nutzen: Plug and Play – easy to use und damit mit wenig Schulungsaufwand
- Geeignet für Einsätze im Personenschutz, im Infrastrukturschutz als auch im Gebietsschutz
- Beliebig vernetzbar, auch mit Geräten zur Abwehr von Gefahren am Boden, zur Bildung eines allumfassenden Perimeterschutzsystems gegen heute bekannte Gefahren am Boden, als auch gegen die neuen Gefahren aus der Luft
- Mandanten- bzw. missionsfähig
- Preisgünstig in der Beschaffung und auch im Einsatz
- Durch hohe Rechnerleistungen und viel Datenablagekapazität aus Cloud-Systemen in geschützten Rechenzentren beliebig skalierbar in Anzahl von Sensoren, Aktoren sowie Geräten für C2
- Umfassende Überwachung und Protokollierung aller Prozesse und Ereignisse in Daten, Text, Ton, Bild oder Video
- Eigenschaften, wie aktuelle 3D-Lagedarstellungen und Künstliche Intelligenz, können flächendeckend zur Verfügung gestellt werden
- Ein Remote-Betrieb als auch ein Report-Support sind jederzeit möglich
- Es ist immer die aktuelle Technik verbunden mit aktuellen Systemdaten und Konfigurationen von Drohnen- und Drohnenabwehrtechnik verfügbar

Eine Drohnensteuerung muss nur für ein bestimmtes Drohnenmodell gebaut werden, ein Drohnenabwehrsystem muss jedoch immer gegen alle am Markt verfügbaren und bekannten Drohnen und Drohnensteuerungen einsetzbar sein. Das ist eine nicht ganz einfache Herausforderung, die technisch und kommerziell nur mit vernetzter IoT-Sicherheitstechnik gelöst werden kann.

Cloudbasierte Sicherheit

Cloud-Computing[4] ist eine IT-Infrastruktur, die beispielsweise über das Internet verfügbar gemacht wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung. Große Clouds verfügen häufig über Funktionen, die von zentralen Servern auf mehrere Standorte verteilt sind.

Cloudbasierte Sicherheit umschreibt den Einsatz von Cloud-Computing für die Sicherheit zugunsten von Personen und Sachwerten. Dabei sind die Cloud-Rechner in Verbindung mit der Datennetzwerktechnik das zentrale Element eines solchen Sicherheitssystems.

Für solche Sicherheitssysteme werden Corporate oder Private Cloud-Systeme eingesetzt, im Gegensatz zu einer Public Cloud, die allen Menschen weltweit zur freien Nutzung offensteht. Die Technik dieser Clouds ist dabei grundsätzlich identisch. Den Unterschied machen die Sicherheitsmaßnahmen zum Schutz der Cloud. Diese Sicherheitsmaßnahmen geben nur den ausgewählten Nutzern und Geräten einen kontrollierten Zugriff auf die Cloud und schränken damit die Flexibilität ein.

Cloud Computing wird normalerweise auf mehrere redundante und gesicherte Rechenzentren an verschiedenen Standorten verteilt. Ein Rechenzentrum, in dem eine Security Cloud gehostet wird, sollte über die entsprechenden Zertifikate zur Einhaltung von internationalen Sicherheits- und IT-Standards verfügen, die da sind:

- Nach Tier-IV-Standard gebaut und zertifiziert
- ISO 27001:2013 für höchste Informationssicherheit
- ISO 50001:2011 für umfassendes Energiemanagement
- ISAE 3402-Typ 2 Prüfbericht
- PCI DSS

Security Cloud-Anwendungen zeichnen sich auch aus durch:

- Hochsichere verschlüsselte Datenübertragung
- Leistungsfähige Firewalls
- Minimierung von Verzögerungszeiten durch spezielle Routing-Konzepte
- Multicastfähigkeit

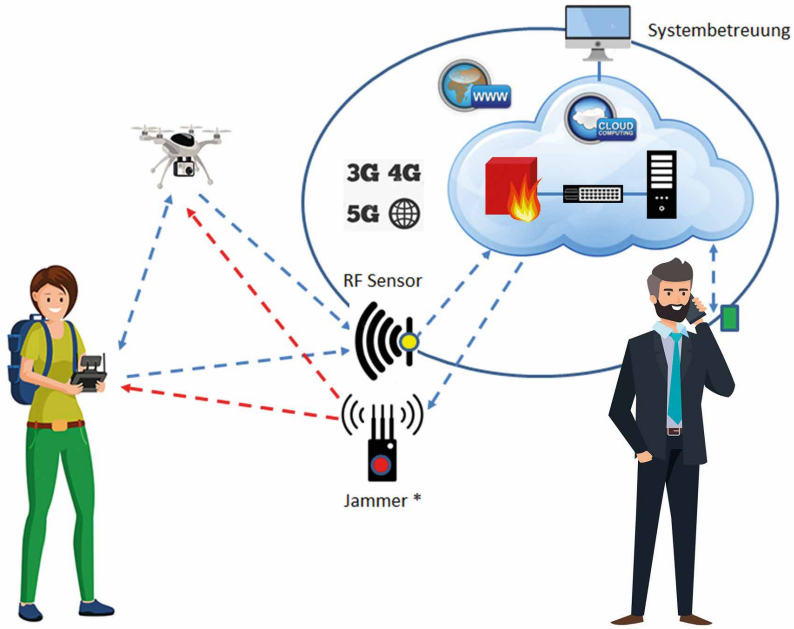

Abbildung: Security Cloud-Anwendung am Beispiel eines Drohnenerkennungssystems für den privaten oder staatlichen Gebrauch durch eine Servicevereinbarung mit einem Sicherheitsanbieter.

- Bereit für Verbindungen verschiedener Systemtechnologien an Sensoren, Aktoren sowie Kommando- und Kontrollstationen (C2)
- Unterstützung aller gängigen Datenübertragungsprotokolle für Daten, Text, Audio, Bild und Video
- Frei skalierbar für Datenablagevolumen und Anzahl an Applikationen
- Fähigkeit, Mandanten und Mission zu trennen, zu verwalten und zu überwachen

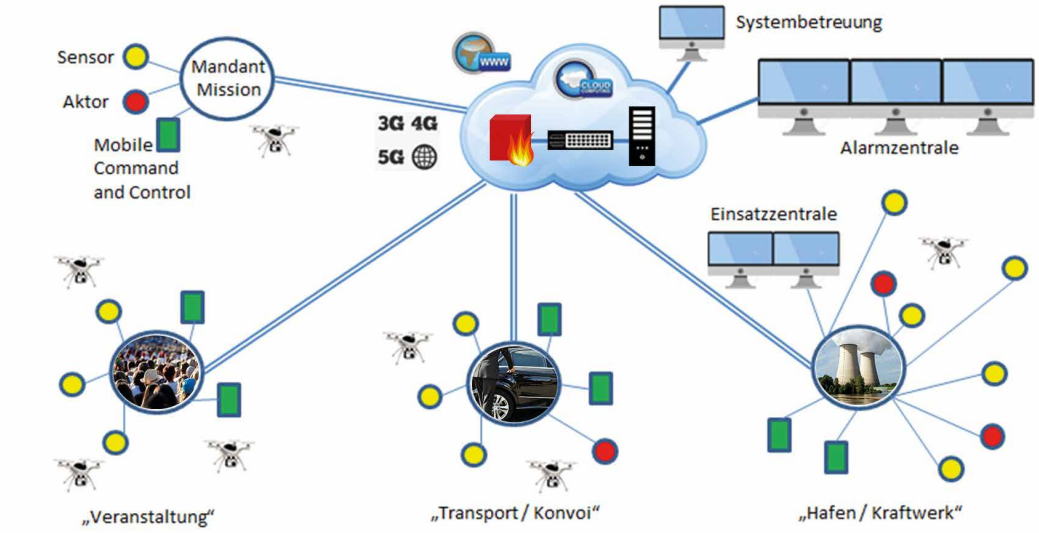

Abbildung: Implementierung von Security Cloud-Anwendungen am Beispiel der Drohnenerkennung und -verteidigung einer privaten Sicherheitsorganisation oder einer Regierungsbehörde mit entsprechenden Funktionen aus Sicht der Security Cloud.

In der Cloud werden alle komplexen technischen Systeme so aufgesetzt, dass die Anwendung im Feld mit den dazu notwendigen Geräten so einfach und so sicher wie möglich erfolgen kann. „Plug and play“ sowie „Easy to use“ bedeuten dabei auch sehr geringen Schulungsaufwand im Feld. Zudem erlaubt die Vernetzung mit der Systembetreuung der Cloud die Benutzer im Feld bei Bedarf remote zu unterstützen und das Gesamtsystem immer auf dem aktuellen technischen Stand zu halten.

Beispiele für cloudbasierte Sicherheitsanwendungen

Cloudbasierte Sicherheit für private Verbraucher

In einer Anwendung für den privaten Gebrauch schließt eine Privatperson ein Service-Agreement mit einem privaten Sicherheitsunternehmen ab. Das Sicherheitsunternehmen stellt danach der Privatperson tragbare RF-Sensoren zur Verfügung. Diese Sensoren kann die Privatperson nun zu Hause, in ihrem Fahrzeug oder an einem beliebigen Ort einsetzen. Über einen kleinen tragbaren Router wird ein RF-Sensor nun über das Mobilfunknetz mit der Security Cloud des Sicherheitsunternehmens verbunden. Dort wird für die Privatperson ein Benutzerkonto eingerichtet und die gesicherte Verbindung mit einem oder mehreren RF-Sensoren aufgebaut. Nun installiert die Privatperson auf einem oder mehreren Smartphones oder Tablets eine App und registriert sich damit mittels Benutzerkonto in der Security Cloud. Damit ist die Anwendung eingerichtet und die Privatperson erhält nun immer eine Warnung, wenn sich Drohnen in der Nähe einer seiner aktiven RF-Sensoren befinden.

Cloudbasierte Sicherheit für Regierungsbehörden

Eine Anwendung für den staatlichen Gebrauch ist im Grundsatz identisch mit dem privaten Gebrauch. Eine Sicherheitsbehörde wie z. B. die Polizei oder das Militär kaufen sich die Sensoren und Aktoren für den Einsatz durch ihre Beamten und die Security Cloud wird in diesem Fall bei der Sicherheitsbehörde eingerichtet und betrieben. Im Gegensatz zur Privatperson können Beamte (Polizisten und Soldaten) auch über die Berechtigung verfügen, tragbare Aktoren gegen Drohneneinsätze zu verwenden. Beispiel eines solchen Einsatzes sind Groß-Ereignisse (Unfall, Naturkatastrophen, Demonstrationen) mit Gaffer-Drohnen, die den Einsatz von Rettungs- und Sicherheitskräften behindern.

Cloudbasierte Sicherheit für mobile Anwendungen

Bei großen Veranstaltungen (Musikfestivals, Sportveranstaltungen im Freien, Demonstrationen, Militärübungen, Polizeieinsätze etc.) werden verlegbare Drohnenabwehrsysteme, eingebaut in Containern oder auf Fahrzeugen, in das zu überwachende Einsatzgebiet gebracht. In diesen Systemen kann auch eine Einsatzzentrale eingebaut sein oder die Sensoren und Aktoren werden über die Security Cloud zur Überwachung und Aktivierung an eine Alarmzentrale aufgeschaltet. Verbunden mit der Security Cloud lassen sich nun auch die Sicherheitskräfte (mit oder ohne tragbare Sensoren und Aktoren) in das System mit einbinden, um bei Bedarf in den Brennpunkt des Geschehens eingreifen zu können.

Cloudbasierte Sicherheit für stationäre Anwendungen

In kritischen Infrastrukturen wie Häfen, Flugplätze, Industrieanlagen, Touristenattraktionen, Energieversorgungs- und Kommunikationseinrichtungen und auch in

großen Überbauungen von Regierungen, Ministerien, Sicherheitsbehörden und Sportorganisationen werden große und leistungsfähige Sensoren und Aktoren fest in der Einrichtung verbaut und über Kabel an eine Stromversorgung und an ein Datennetz angeschlossen. Verfügt die Infrastruktur über eine eigene Einsatz- bzw. Sicherheitszentrale und reicht das kabelgebundene Datennetz von den Sensoren und Aktoren in diese Einsatzzentrale, so werden dort die entsprechenden Drohnenabwehrprogramme eingerichtet und auf die dort vorhandenen Steuerungs- und Kontroll-Bildschirme aufgeschaltet. Verbunden mit einer Security Cloud kann nun die Drohnenlage weiter an die Alarmzentrale der Sicherheitskräfte, welche für die Interventionen und Abwehreinsätze zuständig sind, übermittelt werden.

Abbildung: Verlegbares Drohnenabwehrsystem mit Hochleistungssensoren, -aktoren und eingebauter Einsatzzentrale

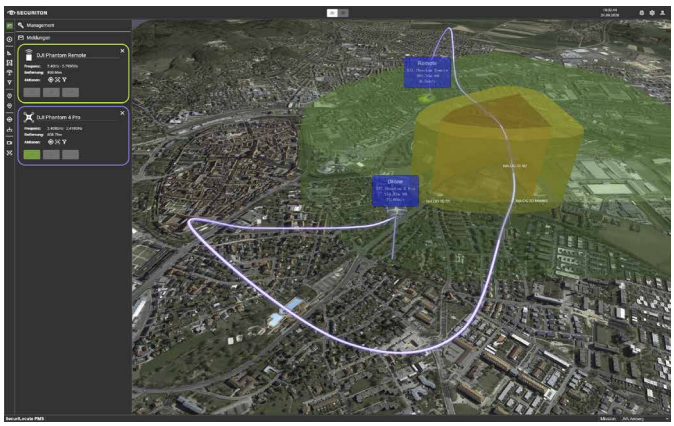

Abbildung: 3D Drohnenlagebild

Flexibilität und Skalierbarkeit von cloudbasierten Sicherheitsanwendungen

Cloudbasierte Sicherheit ist hochflexibel und skalierbar. Sie kann leicht mit den wachsenden Anforderungen des Kunden mitwachsen, sei es für eine Einzelperson, für Gewerbe und Industrie oder für eine Regierungsbehörde. Sowohl mobile als auch statische Sensoren und Effektoren können bei Bedarf integriert werden, auch wenn sie nur vorübergehend zum Einsatz kommen. Cloudbasierte Sicherheit ermöglicht die schnelle Anpassung an eine sich entwickelnde und dynamische Drohnenbedrohung, indem Situationsbewusstsein dort bereitgestellt und verteilt wird, wo es benötigt wird. Und bei Bedarf sowohl zentralisierte als auch dezentralisierte C2-Drohnenverteidigungsmissionen unterstützt werden.

Cloudbasierte Sicherheit bietet auch die Möglichkeit, Sensordaten, Gegenmaßnahmen und Sicherheitspersonal zwischen mehreren am selben Standort befindlichen Infrastrukturen auszutauschen. Große Gewerbe- oder Industriegebiete mit mehreren Unternehmen können gemeinsam ein Drohnenverteidigungssystem mit einer zentralen Schutztruppe einrichten, welches das gesamte Eigentum in dem jeweiligen Gebiet schützt. Der gleiche Ansatz gilt für Regierungsbezirke in Hauptstädten oder großen Logistikzentren, in denen Luft-, Wasser-, Schienen- oder Straßentransportlinien zusammenfließen.

Zusammenfassung

Heutzutage sind Consumer- und kommerzielle Drohnen für jedermann leicht verfügbar und werden immer leistungsfähiger. Dies macht sie zu idealen Instrumenten für Kriminelle und Terroristen, um ihre Fähigkeiten erheblich zu erweitern.

Mit Cloud Computing- und IoT-Technologien können Sicherheitssysteme für die Drohnenabwehr schnell, einfach und überall zu angemessenen Kosten bereitgestellt werden. Auf diese Weise können Drohnenabwehranwendungen über einen langen Zeitraum mit den erforderlichen Diensten und auf einem Leistungsniveau gewartet werden, um mit den rasanten Entwicklungen in der Drohnentechnologie Schritt zu halten.

[1] Remote Identification
https://www.easa.europa.eu/domains/civil-drones-rpas/drones-regulatory-framework-background
[2] IoT Internet of Things
https://en.wikipedia.org/wiki/Internet_of_things
[3] Mobile Monitoring
https://de.wikipedia.org/wiki/Mobile_Monitoring
[4] Cloud-Computing
https://en.wikipedia.org/wiki/Cloud_computing

Securiton Deutschland
Alarm- und Sicherheitssysteme
Hauptsitz: Von-Drais-Straße 33, 77855 Achern, DE
Tel. +49 7841 6223-0, Fax +49 7841 6223-9010
www.securiton.de, info@securiton.de

Ein Unternehmen der Securitas Gruppe Schweiz

SECURITON