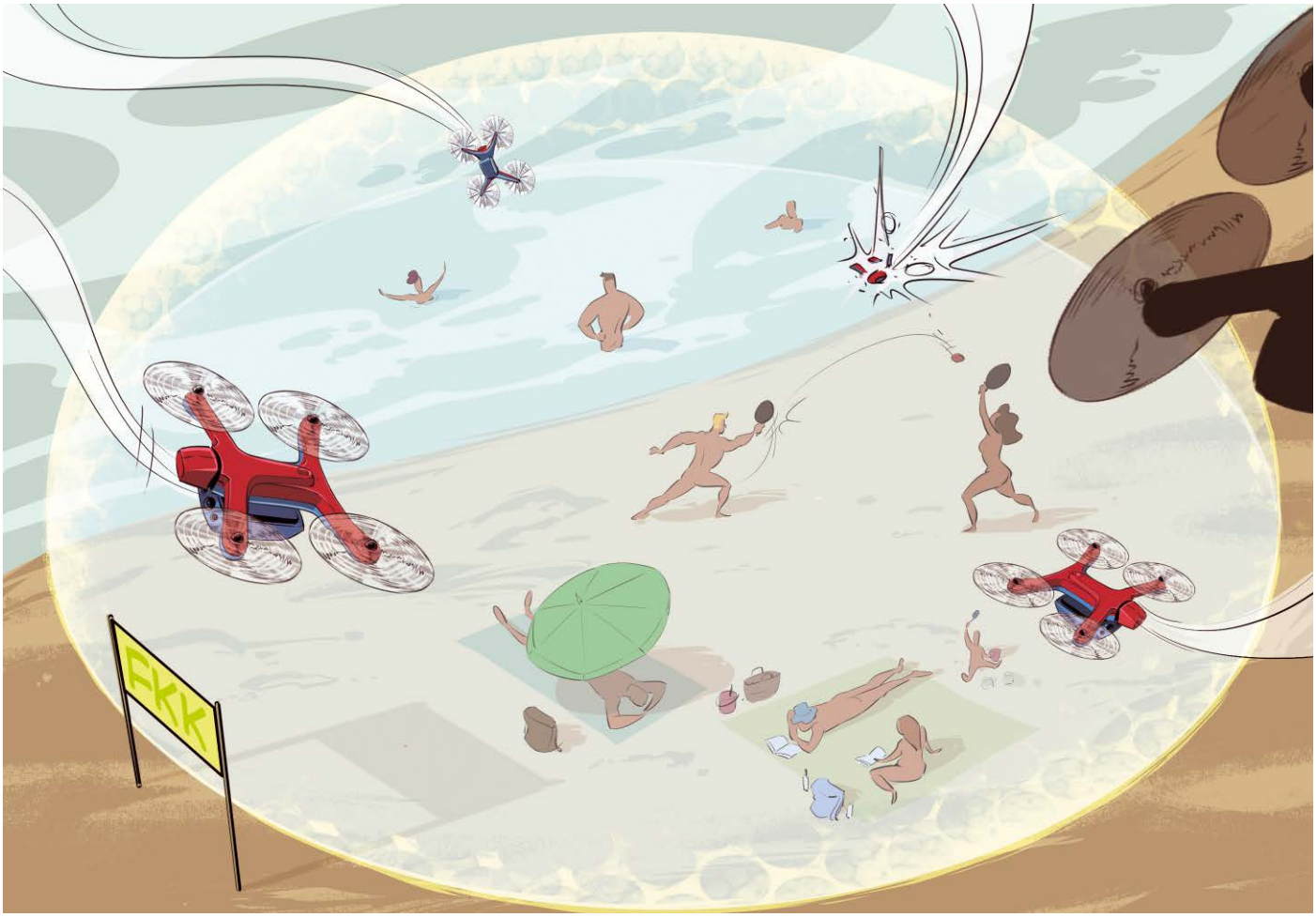

Bild: Albert Hulm

Surrende Gefahr

Forscher im Krieg mit Drohnen

Drohnen sind der Albtraum der Personenschützer und Sicherheitsbehörden. Forschungsprojekte halten mit Störsendern, Netzwerfern und Mikrowellenkanonen dagegen.

Von Arne Grävemeyer

Nach dem Weihnachtsfest nehmen die Drohnenalarme an Flughäfen, Justizvollzugsanstalten oder Bundeswehrstandorten zu, wie Sicherheitsexperten aus Erfahrung wissen. Drohnen sind beliebte Geschenke zum Fest und viele frischgebackene Besitzer wissen gar nicht, wie schnell sie mit ihrem Fluggerät Gesetze überschreiten. Jede Drohnengeneration ist leistungsfähiger als die vorhergehende. Sowohl die Hobbygeräte als auch professionell einsetzbare Drohnen erreichen immer höhere Geschwindigkeiten, längere Flugzeiten und damit höhere Reichweiten bei zunehmenden Traglasten. Selbst Hobbypiloten können ihr Fluggerät mit VR-Brille in First Person View lenken und die Steuerungselektronik unterstützt sie mit halbintelligenten Funktionen wie Ausweichautomatik und selbstständiger Rückkehr zum Startpunkt.

Was da alles möglich wird, treibt Sicherheitsverantwortlichen die Schweißperlen auf die Stirn. Drohnen können Präsentationsvideos drehen oder Industriespionage betreiben, können Medikamente auf ostfriesische Inseln liefern oder Waffen in den Innenhof einer Haftanstalt. Sie könnten sogar einzelne Personen angreifen und Bomben oder Giftstoffe über einer Menschenmenge abwerfen.

Nachdem 2013 bei einer Wahlkampfveranstaltung eine Drohne unangemeldet vor Angela Merkels Nase auf dem Podium landete, verspürte man in einigen Ministerien Handlungsdruck. In der Folge förderte das Bundesforschungsministerium parallel gleich vier Forschungsprojekte, die Mittel gegen Drohnenangriffe im öffentlichen Raum entwickeln sollten, ob in einem Stadion, über dem Volksfest oder eben bei einer Wahlkampfveranstaltung. Die vier Projekte AMBOS, ArGUS, MIDRAS und ORAS verfolgten leicht unterschiedliche Ansätze, um feindliche Drohnen zu erkennen und ihre Angriffe zu stoppen. Im Herbst 2020 ließen sie vor Experten ihre Demonstratoren gegen attackierende Drohnen antreten.

Breites Sensorenspektrum

Da ist das Projekt AMBOS (Abwehr von unbemannten Flugobjekten für Behörden und Organisationen mit Sicherheitsaufgaben), in das neben dem Fraunhofer FKIE (Institut für Kommunikation, Informationsverarbeitung und Ergonomie) und österreichischen Partnern zum Beispiel

auch Praktiker der Polizei ihre Erfahrungen einbrachten. „Der Schlüssel zum Erfolg liegt in der Multimodalität“, sagt Verbundkoordinator Hans Peter Stuch vom FKIE und meint damit die vielfältige Sensorenphalanx und auch ein möglichst breites Arsenal an Gegenmaßnahmen.

Im AMBOS-Projekt setzten die Forscher auf vier Sensortechniken gleichzeitig: Funk, Akustik, Kameras und Radar. Verteilt aufgestellt erkennen die Sensoren angreifende Drohnen lange bevor diese einen definierten Sicherheitsbereich erreichen. Im Demo-Szenario platzierten die Projektpartner den Radardome und ihren Funkempfänger auf dem Dach eines Kastenwagens, in dem sie gleichzeitig ihr zentrales Lagezentrum organisierten. Kameras und Akustiksensoren hingegen verteilten sie an den Rändern des überwachten Bereichs.

Funksensoren mit einer Reichweite über einen Kilometer, bei guten Bedingungen sogar bis zu einer Entfernung von fünf Kilometern, erfassen den Datenaustausch zwischen Fernbedienung und Drohne. Die eingesetzten Funksensoren der Firma Elettronica GmbH peilen die Richtung von Drohne und Pilot. Mehrere Sensoren orten die Positionen von beiden. Akustiksensoren peilen ebenfalls die Richtung, aus der eine Drohne anfliegt und sammeln per Geräuscherkennung sogar weitere Informationen etwa zur Anzahl der Rotoren. Verteilte Akustiksensoren sind ebenfalls in der Lage, die Position einer fliegenden Drohne zu orten, wegen der gegenüber Funk langsameren Schallwellen allerdings nicht so genau wie Funksensoren. Außerdem liegt ihre Reichweite lediglich bei 100 bis 150 Metern.

Als Kameras kombinierten die AMBOS-Projektpartner eine Tageslicht- und eine Infrarotkamera, um auch bei Nacht und Nebel noch Signale erfassen zu können. Die Kameras im Projekt machten anfliegende Drohnen in einer Entfernung von bis zu 1000 Metern aus und halfen bei der Klassifizierung ihrer Größe. Allerdings erlaubt der kombinierte Kamerasensor keine Entfernungsschätzung. Eine große Reichweite hat das Radar, das Drohnen in über 1500 Meter Entfernung ortet.

Im konkreten Fall ist die Kombination der Sensoren entscheidend. Um alle denkbaren Einflugschneisen einer Drohne beispielsweise auf einem Marktplatz in der Stadt zu überwachen, müssen die Sensoren einen Angreifer auch zwischen hohen Gebäuden und in Straßenschluchten aufspüren. Vor dem Radar kann sich eine anfliegende Drohne hinter Gebäuden verstecken und auch Kameras können nicht um die Ecke sehen. Dagegen funktioniert die Funkortung in der Stadt, wenn sie Multipath-Fehler durch Echosignale ausfiltert. Akustiksensoren horchen zusätzlich an jeder Straßenzufahrt die Zufahrtswege ab.

In der Sensordatenfusion und der Lagedarstellung auf einer Umgebungskarte zeigt sich der Mehrwert der AMBOS-Sensorenkombination. Darin implementierten die Forscher einen Multihypothesentracker, der aus den Sensordaten die Geschwindigkeit und Flugrichtung einer Drohne ermittelt. Die Lagedarstellung errechnet dazu, auf welchen Wegen und in welcher Zeit die Drohne den vorgegebenen Sicherheitsbereich erreichen könnte. Daraus ergeben sich die Abwehrmaßnahmen, die das System dem Entscheider vorschlägt.

Vielfältiges Arsenal

Bei AMBOS ist das zunächst einmal ein Störsender (Jammer), der die Nutzsignale zwischen Fernbedienung und Drohne überlagert. Der eingesetzte Jammer der Wüst GmbH hat eine Wirkreichweite von mehr als 1000 Metern. Ohne weitere Steuerungssignale fällt die Drohne in einen Fail-safe-Modus. In der Regel bedeutet das erst einmal, auf der Stelle abwartend zu schweben und nach einer Weile zu landen oder den Rückflug zum Startpunkt anzutreten. Ein Angreifer kann allerdings auch beliebige andere Programme für den Fail-safe-Modus hinterlegen; dadurch ist die Wirkung des Jammer-Einsatzes schwer berechenbar. Beispielsweise könnte eine feindliche Drohne ihre Fracht abwerfen oder auf Kollisionskurs gehen, um sich selbst zu zerstören.

Zudem ist es möglich, dass gar nicht ein Pilot den Angriffsflug steuert, sondern dieser einprogrammiert ist. In diesem Fall kann der Jammer immerhin noch die GPS-Signale zur Satellitennavigation stören. Lediglich eine Drohne mit autarker Trägheitsnavigation kommt dann noch durch.

Es ist theoretisch auch möglich, per Funk mittels Spoofing eine Drohne durch falsche Navigationssignale zu täuschen. Eine mit falschen GPS-Koordinaten gefütterte Drohne findet ihr Angriffsziel nicht und wenn es Sicherheitsverantwortlichen gelingt, eigene Steuerbefehle einzuschleusen, dann landen sie die Drohne zur weiteren Untersuchung in einem gesicherten Bereich. Aber das Spoofing mit Übernahme der Fernsteuerung gelingt heute nur in Einzelfällen unter Laborbedingungen, denn dazu müssen Funkkanäle und -protokolle genau bekannt sein. Als schnell anzuwendende Gegenmaßnahme steht diese Option in absehbarer Zukunft nicht zur Verfügung.

Falls eine Drohne durch die Phalanx der Jammer hindurchgekommen ist, sieht das AMBOS-Modell den Einsatz von HPEM-Effektoren (High Power Electro Magnetics) der Diehl-Gruppe vor. Deren energiereiche Mikrowellenstrahlung induziert in der Steuerungselektronik einer Drohne elektrische Ströme und bringt den Flight Controller durcheinander. Eine derart getroffene Drohne fällt in der Regel wie ein Stein vom Himmel. Da dieser Effekt

Bild: Julian Rothe / Uni Würzburg

Eingenetzt: Im Projekt MIDRAS entwickelten Partner zwei autonom fliegende Drohnen, die Angreifer mit einem Netz vom Himmel holen.

Bild: Jan Woitas / dpa

Der Moment, der die Forschung zur Drohnenabwehr in Wallung brachte: Bei einem Wahlkampfauftritt in Dresden 2013 erhält Kanzlerin Merkel unangemeldeten Besuch von einer Drohne.

über einem Volksfest oder den Zuschauerrängen eines Stadions hochproblematisch ist, können Sicherheitskräfte diese Abwehrwaffen nur an ausgewählten Stellen gezielt einsetzen. HPEM-Effektoren wirken auf 100 bis 200 Meter, sind aber aufgrund ihrer unspezifischen Wirkung auf kurze Distanz auch gegenüber Mensch und Tier nicht ungefährlich.

Als Ultima Ratio sieht das AMBOS-System Netzwerfer am Boden vor, die ein Netz mit Gewichten etwa hundert Meter weit auf eine anfliegende Drohne schießen können. Diese Netzwerfer erwiesen sich während des Projektzeitraums aber noch nicht als verlässliche Schutzmaßnahme, da sie sich zwar auf die anfliegende Drohne ausrichten können, mit steigender Einsatzhöhe und -entfernung aber zum Beispiel windanfällig reagieren. Ihr Einsatz ist damit schwer zu berechnen.

Zwei Drohnen mit Fangnetz

Eine effektivere Variante hat eine Forschungsgruppe der Universität Würzburg im Rahmen des Verbundprojektes MIDRAS (Mikro-Drohnen-Abwehr-System) entwickelt. Das Team programmierte zwei Drohnen so, dass sie eine Angreiferdrohne mit einem zwischen ihnen aufgehängten Netz einfangen. Die Würzburger Drohnen sind darauf ausgelegt, nicht nur autonom in Formation, sondern sogar physisch durch das Netz miteinander gekoppelt zu fliegen und den Einschlag einer gegnerischen Drohne in ihrem Fangnetz rasch zu kompensieren. Auch bei dieser Lösung stürzt die eingefangene Drohne nicht auf Personen herunter und die Polizei kann sie später auf Fingerabdrücke, gefährliche Fracht oder Daten untersuchen.

Allerdings bilden die beiden Würzburger Drohnen mit ihrem Netz ein robustes System, das insgesamt satte acht Kilogramm wiegt. Dessen Wendigkeit ist eingeschränkt, eine schnelle Drohne mit Ausweichautomatik oder eine geschickt gesteuerte Drohne kann einem solchen Ungetüm entkommen. Daher setzte auch das MIDRAS-Projekt zur Unterstützung zusätzlich auf den Einsatz von Störsendern.

Ganz auf die Detektion unbemannter Flugsysteme in Städten konzentrierte sich das Verbundprojekt ORAS (Sensorgestütztes Überwachungs- und Alarmierungssystem). Da man davon ausgeht, dass im Stadtgebiet eine angreifende Drohne unter dem Radarschirm fliegt, haben die Projektpartner zusätzlich eine Reihe optischer Kameras mit Tageslicht- und Infrarotsensoren vorgesehen. In diesem Fall dienen die untersuchten Radarsysteme vor allem dazu, die Kameras einzuweisen.

Bild: Fraunhofer FKIE

Das AMBOS-Lagezentrum zeigt die anfliegende Drohne an sowie die einsetzbaren Jammer, Mikrowellenkanonen und Netzwerfer; es schätzt zudem die Erfolgsaussichten der Maßnahmen ein.

Im Rahmen des ORAS-Projektes trainierten die Entwickler ein Radarsystem der Spinner GmbH darauf, Dopplerinformationen zu nutzen, um eine angreifende Drohne von Vögeln und anderen Falschzielen zu unterscheiden. Mit Kameras der Intenta GmbH gelang es, die anfliegende Drohne, sobald diese einmal durch die optischen Sensoren erfasst war, anhand ihrer Signatur im weiteren Flug zu verfolgen. Ihr Bild übermittelten die Systeme als stabilisierten Livestream, hoch aufgelöst mit Informationen über die Flugbewegung zur Leitstelle.

Angriffsszenarien vorhersehen

Die Analyse eines Drohnenangriffs und der Vorschlag zeitlich sinnvoller Gegenmaßnahmen bilden die Kernelemente des ArGUS-Projektes unter Verbundkoordinator Dr. Gunther Grasemann vom Fraunhofer IOSB (Institut für Optronik, Systemtechnik und Bildauswertung). Ziel ist es, dem Sicherheitsverantwortlichen realistische Handlungsempfehlungen zu geben und so die Reaktionszeit zu senken. Bei diesem Projekt waren Anwender wie etwa der Sicherheitsdienstleister des Hamburger Volksparkstadions und die Fraport AG als Betreiber des Frankfurter Flughafens mit im Boot.

Ähnlich wie beim AMBOS-Projekt setzt auch ArGUS auf Multisensorik und erstellt einen Lageplan, der die Drohne und ihre Flugrichtung darstellt. Darüber hinaus nutzt das ArGUS-Projekt die Sensordaten, insbesondere die Funksensoren, um den Drohnentyp zu identifizieren, womit sich beispielsweise deren Maximalgeschwindigkeit und Traglast abschätzen lassen. Dabei kommt ein an der TH Deggendorf entwickeltes Software-Defined-Radio-System zum Einsatz, das die Funkverbindung zwischen Angreiferdrohne und Fernbedienung abhört und daraus den Drohnentyp ermittelt. Die Beschaffungskosten dieser Komponente liegen voraussichtlich deutlich niedriger als bei bisherigen Funksensoren.

Zudem haben die Projektpartner gemeinsam mit den Anwendern in Workshops denkbare Angriffsszenarien durchgespielt. Wilfried Joswig, Geschäftsführer des Verbands für Sicherheitstechnik (VfS) berichtet: „Am Anfang meinten die Verantwortlichen eines Industriebetriebs zum Beispiel, das Thema sei für sie überhaupt nicht relevant. Aber am Ende des Workshops hatten wir für genau diesen Betrieb 150 Angriffsszenarien erkannt, von der

einfachen Industriespionage bis zu böswilligen Attacken, Sabotage oder Terror."

Das ArGUS-Projekt sammelt Angriffsszenarien eines Einsatzortes gemeinsam mit möglichen Gegenmaßnahmen in einer Datenbank. „Die Zahl der Szenarien wächst schnell, allein in einem Stadion kommen leicht hunderte Varianten zusammen", schildert Grasemann. Man denke nur an einen Besuch der Kanzlerin bei einem Fußballspiel. In dem Fall geht es nicht mehr nur darum, Attacken auf Sportler und Zuschauer zu verhindern, sondern zusätzlich um den Prominentenschutz.

Bild: Fraunhofer FKIE

Mit Störsignalen überlagert der Jammer die Funkverbindungen einer Drohne, sodass sie weder Steuersignale noch Navigationsdaten erhält.

Bild: Fraunhofer FKIE

Zielgerichtete Mikrowellenstrahlung erzeugt elektrische Ströme und setzt damit die Steuerungselektronik einer angreifenden Drohne außer Gefecht.

Weiche und harte Maßnahmen

Schnell wird klar, dass Einsatzort, Art der Veranstaltung, Angriffsszenario und Gegenmaßnahmen eng miteinander verknüpft sind. Dementsprechend lassen sich konkrete Gegenmaßnahmen planen. Die beginnen bei passiven Schutzmaßnahmen, etwa dem frühzeitigen Aufspüren des Drohnenpiloten. Gegen Industriespionage hilft es, technische Neuentwicklungen abzudecken oder den Firmenhof zu vernebeln, und als Schutz gegen einen Anschlag im Stadion führt man die Kanzlerin hinter eine Seitentür.

Darüber hinaus berücksichtigt ArGUS zunächst die weichen Maßnahmen. Darunter verstehen die Partner das Jamming und falls möglich auch das Spoofing, voraussichtlich mit falschen GPS-Daten.

Schließlich bilden harte Abwehrmethoden eine Option, wenn es die Gefährlichkeit der Drohne und des denkbaren Angriffsszenarios erfordern. Diese Maßnahmen stoppen eine Drohne physisch. In dieser Kategorie sieht das ArGUS-System Schnittstellen zu Mikrowellen-Effektoren vor, zu Wasserwerfern, Netzwerfern von handgetragenen oder bodenstationierten Systemen sowie Abfangdrohnen mit Netz. In der Theorie sind überdies beispielsweise starker Schall, Laser, Flammenwerfer oder Schusswaffen vorstellbar, allerdings sind derartige Maßnahmen in der Öffentlichkeit wohl nicht genehmigungsfähig.

Derzeit nicht weiter verfolgte Gegenmaßnahmen sind etwa Abfangdrohnen in Form von Kamikazejägern. Abgesehen von der Gefahr, dass bei Erfolg gleich zwei Drohnen unkontrolliert herabstürzen, befinden sich derartige Lösungen noch nicht einmal im Experimentierstadium – die technischen Anforderungen sind einfach zu komplex. Für Aufmerksamkeit sorgten bereits dressierte Greifvögel, die anfliegende Drohnen fangen. Ein solches Vorgehen sei aber auch eine Frage des Tierschutzes, sagt Hans Peter Stuch. Zudem haben solche Tiere in Versuchen einen eigenen Willen bewiesen: Wenn sie keine Lust haben, fangen sie eine Drohne eben nicht ab.

Das Beste vom Besten

Die gezeigten Einzellösungen vermarkten die Industriepartner bereits in Eigenregie. Wie die Forschungsprojekte aber zeigen, liegt der Schlüssel zum Erfolg vor allem in der abgestimmten Gesamtlösung mit vielfältiger Sensorik, zentraler Analyse und Lagedarstellung sowie dem Zugriff auf ein möglichst breites Arsenal an Gegenmaßnahmen. Wie Insider berichten, arbeiten Partner der vier Projekte AMBOS, ArGUS, MIDRAS und ORAS in den kommenden Wochen daran, ein Leuchtturmprojekt aufzubauen, das die erfolgreichsten Komponenten zusammenfasst und diese zu einer Gesamtlösung mit Produktreife zu Ende entwickelt.

„Eine Art Cherry Picking aus den besten Komponenten der gezeigten Systeme", nennt Stuch dieses Projekt. „Diese Initiative wird Einzelmodule zusammenstellen, die günstiger, leichter zu handhaben oder schneller einzusetzen sind als heutige Lösungen auf dem Markt", sagt Christian Jaeger voraus. Der ESG-Geschäftseinheitsleiter ist zuständig für Drohnendetektion und -abwehrsysteme und war am MIDRAS-Projekt beteiligt. Als Ergebnis erwartet er in den kommenden drei Jahren eine marktreife Gesamtlösung mit hoher Sensordatenfusion, darauf aufbauender ausgereifter Drohnenklassifizierung und einer sehr schnellen Entscheidungsunterstützung für den Verantwortlichen. *(agr@ct.de)* **c't**

Weitere Infos: ***ct.de/yfps***

Bild: Fraunhofer FKIE

Netzwerfer am Boden schleudern Fangnetze bis zu 100 Meter weit.