Drohnenabwehrsystem: Der Schlüssel für Abwehrmaßnahmen liegt darin, die Drohnen frühzeitig zu erkennen.

Gefahren durch Drohnen und Autos

Beim Perimeter-Protection-Kongress 2018 in Nürnberg berichteten Experten über Gefahren durch Drohnen und Terrorangriffe mit Kraftfahrzeugen und informierten über Maßnahmen und Strategien.

Der Perimeter-Protection-Kongress, organisiert vom *Verband für Sicherheitstechnik e.V. (VfS)*, fand messebegleitend an den beiden ersten Tagen der Fachmesse „Perimeter Protection" statt, die vom 16. bis 18. Jänner 2018 im Messezentrum Nürnberg abgehalten wurde. Pro Tag wurden den rund 150 Teilnehmern in drei Blöcken sechs Referate von 45 Minuten Dauer geboten, mit anschließender Diskussion.

Drohnen. Markus Piendl, Sachverständiger für Sicherheitstechnik, brachte Beispiele, wie durch den Einsatz von Drohnen *(Unmanned Aerial Vehicles – UAVs)* Industriespionage betrieben oder in Persönlichkeitsrechte eingegriffen wird. „Beträge im fünfstelligen Bereich werden bezahlt, um Bilder von der Testfahrt eines in Entwicklung stehenden Automodells zu erhalten. Gegen Bezahlung werden Video-Streams von FKK-Stränden übermittelt." Drohnen, die etwa 500 Euro kosten, reichen dafür aus.

Bei Sportveranstaltungen, die von Drohnen gefilmt werden, wird in Übertragungsrechte eingegriffen. Über vollbesetzten Stadien weißes Pulver zu zerstäuben, könnte Panik auslösen. Wenn sich Drohnen im gesperrten Luftraum von Flughäfen aufhalten und Flugzeuge deshalb umgeleitet werden müssen, stellt sich die Frage, wer die dadurch entstehenden Kosten trägt – die Fluglinie, der Flughafen oder der Staat? Drohnen stellen eine Gefahr für Betriebe der kritischen Infrastruktur dar. Ziele für Drohnenangriffe könnten auch Kommunikationseinrichtungen auf Hochhäusern oder Richtfunkstrecken sein.

Der Schlüssel für Abwehrmaßnahmen liegt darin, die Drohnen frühzeitig zu entdecken. Bei einem Feldversuch mit Detektionssystemen von 25 Anbietern wurde diese Aufgabe von allen gelöst, mit unterschiedlichen Reichweiten. Wichtig wäre auch, den Piloten zu finden sowie eine Freund-Feind-Kennung einzuführen, um die eigene Drohne von anderen unterscheiden zu können. Wie im übrigen Luftverkehr, sollten Drohnen mit Transpondern ausgestattet sein. Dritte dürfen durch Abwehrmaßnamen nicht gefährdet werden. Elektronische Abwehrmaßnahmen (Jammen) sind der Behörde vorbehalten.

„Eine hohe Wahrscheinlichkeit eines Missbrauchs besteht bei Drohnen, die in der Preisklasse ab etwa 500 Euro liegen und von Hobby-Piloten geflogen werden", sagte Dr. Gunther Grasemann, *Fraunhofer IOSB, Karlsruhe (www.iosb.fraunhofer.de)*. Er unterteilte das Missbrauchspotenzial in bloße Störungen („Kinderstreiche", Ausspähung), Gesetzeswidrigkeiten (Fliegen in Flugverbotszonen; Transport von gefährlichen Objekten) und Gefährdungen, etwa durch Anschläge auf Personen oder die Infrastruktur. Während Anschläge gegen eine bestimmte Person eine präzise Steuerung der Droh-

FOTO: KURT HICKISCH

ne voraussetzen, fällt bei terroristischen Angriffen dieses Erfordernis weg.

Ansatzpunkte zur Verhinderung von Drohnen-Angriffen ergeben sich aus den einzelnen Phasen des Einsatzes. Der Angriff muss vorbereitet und die Ausrüstung beschafft werden. Es erfolgt der Anflug, die Einwirkung am Zielort, die Landung und die Nachbereitung (Rückbau, Spurenbeseitigung, Abtransport).

Experten von *Fraunhofer IOSB* haben zur schnellen Detektion und Klassifikation anfliegender Drohnen das „Modulare Drohnenerfassungs- und Assistenzsystem“ (MODEAS) entwickelt. Es detektiert Drohnen multisensoriell (optisch, akustisch, funktechnisch). Die einzelnen Stationen (Module) vernetzen sich automatisch und kalibrieren sich wechselseitig, was eine präzise Ortung ermöglicht. Kommunikationstechnisch könnte auf die Fernsteuerung der Drohne eingewirkt werden (Signale manipulieren oder unterdrücken), auf den Autopiloten (Übertragung falscher Werte), auf den GPS-Sensor (Manipulieren oder Unterdrücken des Signales) und Einflussnahme auf die Visualisierung bzw. Videoübertragung.

Mögliche „sanfte“ Abwehrmaßnahmen, die in der Regel nicht zur Beschädigung oder dem Absturz der Drohne führen, wären Blendung der Kamera, etwa mit einem Laser, Störung der Kommunikation/Navigation („Jamming“), Verfälschung des GPS-Signals („Spoofing“) oder Übernahme der Kontrolle. „Harte“ Maßnahmen zur Abwehr direkter Gefährdungen wären die Beschädigung elektronischer Komponenten mit energetischer Einwirkung, Verursachen der Flugunfähigkeit (Kleber, Leine), Abfang (mit anderen Drohnen oder bemannten Fluggeräten) oder Abschuss (Wasserstrahl, Laser, Feuerwaffen).

Elektronische Abwehrmaßnahmen gegen Drohnen wie Jammer dürfen nur von Behörden eingesetzt werden.

Grasemann berichtete über das Forschungsprogramm des BMBF *ArGUS,* das „Assistenzsystem zur situationsbewussten Abwehr von Gefahren durch UAS“. Neben dem IOSB, der Johannes-Gutenberg-Universität Mainz und Industrieunternehmen sind für Praxistests auch der Flughafen Frankfurt sowie das LKA Bayern und das BKA eingebunden. Es sollen die Anforderungen an Drohnendetektionssysteme definiert und Parameter für entsprechende Datenbanken erarbeitet werden.

Rechtsfragen. Bei der Detektion von Drohnen werden Daten durch Sensoren erfasst, gespeichert, miteinander kombiniert und mit Datenbanken abgeglichen. Daraus ergeben sich grund- und datenschutzrechtliche Probleme, indem in Persönlichkeitsrechte eingegriffen wird. Laut Johannes Marosi von der Johannes Gutenberg-Universität Mainz stelle sich bei akustischen und optischen Sensoren das Problem des „Beifangs“, dass Stimmen oder Bilder von erkennbaren, unbeteiligten Personen aufgenommen werden, was auf eine Überwachung des öffentlichen Raums hinauslaufe. Bei „sofortiger“ Aussortierung liege keine Grundrechtsverletzung vor. Unproblematisch sei in dieser Hinsicht die Radardetektion. Die Verwendung mehrerer Sensoren, die Vernetzung und das Tracking von Objekten gehe in den Auswirkungen über übliches Beobachten hinaus.

Das Fernmeldegeheimnis (Art. 10 GG, Art. 10a StGG) schützt die Vertraulichkeit der unkörperlichen Übermittlung von Bildern, Tönen und sonstiger Daten mit Hilfe von Fernmeldeeinrichtungen. Die Schutzwürdigkeit liege darin, dass die Beteiligten ihre Daten einem Dritten zum Transport anvertrauen. Die Datenübermittlung zwischen dem UAS erfolge allerdings direkt und nicht über das Telekommunikationsnetz eines Dienstleisters. Sie verbleiben im Herrschaftsbereich des Betreibers. Anders im Telekommunikationsrecht. Der Begriff der Telekommunikation sei rein technisch, setze keinen Datenaustausch zwischen Menschen voraus, Signale müssten nicht über das Netz eines Dritten übertragen werden.

Die Kommunikation zwischen dem UAS und der Fernsteuerung falle unter den Begriff Nachricht, sobald ein Informationsgehalt (Steuerung) übermittelt werde, wobei erkennbar ein nicht öffentlicher Datenübertragungsvorgang stattfinde. Das Abfangen von Daten ist in Deutschland nach § 202b dStGB strafbar, in Österreich käme § 119a StGB (Missbräuchliches Abfangen von Daten) in Betracht.

Dem Datenschutz unterliegen nach Art. 4 Nr. 1 DSGVO Informationen, die sich auf identifizierte oder identifizierbare Personen beziehen. Identifizierbarkeit ist gegeben, wenn eine Person mit Mitteln, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, identifiziert werden kann (Erwägungsgrund 26 DSGVO). In Betracht kommen können unter anderem GPS-Koordinaten, wenn sie den Aufenthaltsort einer bestimmbaren Person beschreiben, Identifizierungssignale über Transponder sowie die Video- und Audioaufnahmen.

Bei hoheitlichem Handeln bedürfen Eingriffe in Grundrechte einer einfachgesetzlichen Regelung, bei der der Grundsatz der Verhältnismäßigkeit eingehalten werden muss. Kriterien für die Schwere des Eingriffs bei Überwachungsmaßnahmen sind laut Marosi die Sensibilität und Aussagekraft der erfassten Daten, die Streubreite des Eingriffs und die Heimlichkeit der Maßnahme. Es gebe (in Deutschland in den Landespolizeigesetzen) zwar Ermächtigungen zur Verwendung einzelner Sensoren eines Detektionssystems (Videoüberwachung, Tonaufzeichnungen, Datenabgleich), aber keine, die sämtliche Sensoren abdecke. Vernetzte Systeme und vermutlich auch Tracking würden Ergänzungen der bestehenden Ermächtigungen erfordern.

Bei der Abwehr von Drohnen liege, wenn entweder die Drohne oder das Eigentum Dritter beschädigt wird, ein Eingriff in das Grundrecht auf Eigentum

FOTOS: KURT HICKISCH

vor. Hoheitliche Abwehrmaßnahmen müssten sich, soweit sie in Grundrechte eingreifen, auf entsprechende Ermächtigungen stützen können.

Das Jammen der Funkverbindung zu einem UAS sei insofern ein schwererer Eingriff als das Blockieren von Mobilfunkverbindungen, als die Gefahr eines Drohnenabsturzes und eines Schadens für Dritte bestehe sowie, dass möglicherweise Funkverbindungen (Flughafen) gestört werden. Der Einsatz von Netzwerfern oder HPEM-Wellen scheine bisher gesetzlich noch ungeregelt zu sein.

Bei Privaten könnten bei bloßen Überflügen Persönlichkeitsrechte wie das Recht am eigenen Bild betroffen sein, Geschäftsgeheimnisse oder das Hausrecht; bei drohenden Abstürzen oder Anschlägen die Grundrechte auf körperliche Unversehrtheit oder Eigentum.

Als Rechtsgrundlage für Abwehrmaßnahmen kommen Notwehr oder Notstand in Betracht, die allerdings voraussetzen, dass ein Schaden unmittelbar bevorstehen muss, schon eingetreten oder zumindest hinreichend wahrscheinlich ist.

Soweit möglich, ist staatliche Hilfe in Anspruch zu nehmen. Notwehrmaßnahmen sind zur bloßen „Unfugabwehr“ (§ 3 Abs. 1 2. Satz StGB) nicht gerechtfertigt. Notstand (§ 10 StGB) entschuldigt nur dann, wenn der aus der Tat drohende Schaden nicht unverhältnismäßig schwerer wiegt als der abzuwendende Nachteil. Funkstörer dürfen von Privaten nicht betrieben werden. Für schuldhafte rechtswidrige Abwehrhandlungen besteht Haftung nach Zivilrecht.

Terrorangriffe mit Kraftfahrzeugen. „Nutzfahrzeuge sind die effektivste Terrorwaffe“, stand in der Online-Ausgabe des IS-Magazins „Rumiyah“ nach dem Anschlag in Nizza am 14. Juli 2016 mit 86 Todesopfern. In der Folge ereigneten sich die Terroranschläge mit Kraftfahrzeugen in Berlin am 19. Dezember 2016, in Stockholm am 7. April 2017 und in Barcelona am 17. August 2017.

Temporärer Zufahrtsschutz *Truckbloc.*

Christian Schneider, Fachmann für Zufahrts- und Steinschlagschutz, gründete nach dem Anschlag auf den Weihnachtsmarkt in Berlin am 19. Dezember 2016 die „Initiative Breitscheidplatz“, um dazu beizutragen, Veranstaltungen vor Angriffen mit Kraftfahrzeugen zu schützen. Nach einem Urteil des BGH vom 3. Februar 2004, Az VI ZR95/03, darf „der Besucher darauf vertrauen, dass ihm nichts passiert“.

Gesetzliche Vorgaben bestehen in der Verkehrssicherungspflicht und der Sorgfaltspflicht, die sich bei Fahrzeugsperren in der ISO IWA 14 Serie näher konkretisieren. Diese wurde durch ein internationales Expertengremium aus 34 Ländern und Organisationen erarbeitet und stellt die international anerkannten Regeln der Technik dar. Sie gilt seit 15. November 2013 und wird alle fünf Jahre aktualisiert.


VfS-Vorsitzender Wilfried Joswig: Moderator der Referate beim Perimeter-Protection-Kongress.

Teil 1 der Norm (IWA 14-1) ist die Prüf- und Zulassungsrichtlinie für Zufahrtsschutzbarrieren, sowohl stationäre als auch mobile, definiert deren Leistungskriterien und regelt detailliert die Prüfmethoden und den Crash-Test.

Die IWA 14-2 ist die umfassende Anwendungsrichtlinie. Sie definiert den Prozess zur lokalspezifischen Gefährdungsbeurteilung, bewertet die Einsatzfähigkeit von zertifizierten Barrieren, fordert die Qualifikation der Benutzer und regelt die Wartung der Barrieren.

Das Schutzkonzept nach IWA 14-2 wird in sechs Schritten erstellt: Gefährdungsbeurteilung (Was ist wann vor welcher Gefahr zu schützen?), Bedrohungsszenarien (Wo könnte mit welchen Fahrzeugen ein Angriff erfolgen?), Einsatzanforderungen (Fluchtwege freilassen, keine Sichtbehinderung, Art der Barrieren), technische Umsetzbarkeit vor Ort (Eignung der Barriere bei den gegebenen Verhältnissen), Erstellen des Zufahrtsschutzkonzeptes sowie Abnahme und anhaltende Funktionsfähigkeit. „Angreifer aussperren, ohne das Publikum einzusperren“, betonte Schneider.

Bei stationären Sperren ist die *Dispersion* zu beachten: Abgerissene Primärteile und Ladung fliegen in die Menge. Die Gefahr bei mobilen Sperren liegt in der *Penetration* insofern, als das Fahrzeug nicht abrupt aufgehalten, sondern abgebremst wird und dementsprechend aus diesem Grund ein (berechenbarer) Sicherheitsabstand zu dem zu schützenden Bereich einzuhalten ist. Ein temporärer Zufahrtschutz ist *TruckBloc (www.truckbloc.com)*.

DI Matthias Demmel, Prüfzentrum für Bauelemente – PfB in Rosenheim, berichtete über die praktische Durchführung der Prüfung der Einbruchssicherheit nach den Normen EN 1627 – 1630. Die für die Perimetersicherung wichtigen Tore sind von der EN 1627 ausgeschlossen. An der Zuordnung elektromechanischer Verschlüsse an Türen sowie mechatronischer Schlösser wird gearbeitet.

Über Anforderungen und Entwicklungen in der Perimetersicherung referierte Prof. Dr. Ing. Andreas Hasenpusch. Er informierte über die Gefährdungen (auch durch Terror und Drohnen), die an die Perimetersicherung zu stellenden Anforderungen, die Möglichkeiten zu deren technischer Umsetzung und den derzeitigen Stand von Wissenschaft und Forschung samt den absehbaren technischen Entwicklungen, wie etwa mit dem Projekt *ArGUS*. *Kurt Hickisch*

www.perimeter-protection.de

FOTO: KURT HICKISCH