NICHT-MILITÄRISCHE DROHNENABWEHR

ZUSAMMENFASSUNG

Die rasante Entwicklung der Drohnentechnologie hat zu zivilen Anwendungen in Bereichen wie Forschung, Logistik und Sicherheit geführt. Unbemannte Luftfahrzeuge (UAVs) werden zunehmend auch in der Landwirtschaft, Logistik oder zur Freizeitgestaltung eingesetzt. Sie spielen aber auch eine entscheidende Rolle in der modernen Kriegsführung. Diese Verbreitung wirft Sicherheitsbedenken auf, da Drohnen für Spionage und terroristische Aktivitäten missbraucht werden können. Technologien zur Erkennung und Neutralisierung von Drohnen sind unerlässlich, um diese Risiken zu mindern. In Österreich ist der zivile Drohnenbetrieb durch EU-Richtlinien geregelt und wird von mehreren staatlichen Stellen überwacht. Ein kontinuierliches Monitoring der technischen Entwicklungen ist unerlässlich, um den sich ständig weiterentwickelnden Herausforderungen der UAV-Technologie gerecht zu werden.

ÜBERBLICK ZUM THEMA

Drohnen entwickeln und verbreiten sich rasch, auch im zivilen Bereich

Umgangssprachlich wird der Begriff „Drohne“ für militärisch oder kommerziell genutzte, unbemannte Luftfahrzeuge verwendet. In der wissenschaftlichen Praxis hat sich die Bezeichnung „Unmanned aerial vehicle“ (UAV) etabliert. Im zivilen Kontext werden UAVs u. a. in der Forschung, Logistik (siehe ***Lieferdrohnen***), Landwirtschaft, Forstwirtschaft sowie durch Sicherheitsunternehmen, von verschiedenen Behörden (z. B. Polizei und Feuerwehr, siehe ***Sicherheits-Robotik***, ***Waldbrände***) und als Freizeitbeschäftigung genutzt. Speziell „Commercial of the shelf“ (COTS) UAV-Systeme und -Komponenten haben eine breite Verwendung gefunden. Die verfügbaren Modelle mit HD/4K/8K-Kamera, GPS-Steuerung und einer Signalreichweite von bis zu neun Kilometern, sowie einer Flugzeit von bis zu 40 Minuten werden in einer Preisspanne von ca. 100 € bis 4.000 € angeboten. Auch handelsübliche Drohnen verfügen inzwischen über weitreichende Autonomiefähigkeiten – wobei Flüge ohne Sichtkontakt von Privaten ohne Lizenz nicht zulässig sind. Ein Autopilot sorgt meist dafür, dass das Luftfahrzeug stabilisiert wird, und steuert die Ausrichtung, Position und Geschwindigkeit der Drohne. Überdies können autonome Systeme dafür sorgen, dass das UAV bei einem Ausfall der Kommunikation selbstständig den Weg zurück zur Basis findet oder sicher landet. Bei vollautonomen UAVs müssen schließlich nur mehr verschiedene Parameter vorgegeben werden, damit die Drohne die gestellte Aufgabe selbstständig erfüllt.

Das Missbrauchspotenzial von Drohnen ist im zivilen Bereich sehr hoch

Durch den vermehrten Einsatz von UAVs entstehen unweigerlich neue Herausforderungen für die zivile Sicherheit (Del Re, et al., 2024). Unfälle oder Gesetzesüberschreitungen mit UAVs passieren nicht selten unabsichtlich. Oft können diese Vorfälle gravierende Folgen haben. Beispielsweise verursachten in der Nähe von Flughäfen fliegende Drohnen schon mehrmals Flugausfälle, die Millionenschäden nach sich trugen. Viele COTS-UAVs verfügen daher über Systeme, die Flugverbotszonen automatisch erkennen und entweder den Piloten warnen oder die Drohne daran hindern, in diese Zonen einzufliegen. Bei intentionalem Missbrauch von UAV-Technologien helfen solche Systeme aber wenig. Da das System mit GPS arbeitet, lässt es sich einfach umgehen, beispielsweise indem man die GPS-Erkennung des UAVs deaktiviert. Durch die Kombination mit anderen Technologien können Drohnen zudem mit neuen schädlichen Funktionalitäten ausgestattet werden, das Missbrauchspotenzial ist somit sehr hoch. Einige bemerkenswerte Innovationen durch Privatpersonen sind unter anderem die Modifizierung einer Drohne zur Sammlung von Daten oder zur Bewaffnung. Ausprobiert wurde das Abfeuern einer Handfeuerwaffe oder eines Flammenwerfers, die an einer Drohne befestigt wurden. Zudem wurden Spraydosen an Drohnen angebracht, um großflächig Werbeplakate zu besprühen (Rassler, 2016).

Spionage

Drohnen werden zunehmend zur Spionage eingesetzt, wie verschiedene Vorfälle zeigen. Mit videofähigen UAVs können kritische Infrastrukturen, Personen oder Organisationen ausgespäht werden, um das erbeutete Bild- und/oder Videomaterial für private, wirtschaftliche oder strategische Zwecke auszunutzen. UAVs können zusätzlich zu den Kameras mit anderen komplexen Sensoren ausgestattet sein und so sensible Informationen, wie z. B. Telekommunikationsdaten, stehlen. In den letzten Jahren wurden in Deutschland mehrfach militärische Einrichtun-

gen und Firmengelände durch Drohnen ausgespäht, das genaue Ausmaß ist unbekannt.[1] Andere Vorfälle demonstrieren das Potenzial, Drohnen für terroristische Zwecke einzusetzen. So ließ Greenpeace 2018 zwei UAVs in ein französisches AKW abstürzen, um die Anfälligkeit von Atomkraftwerken für terroristische Angriffe zu demonstrieren. Im Jahr 2015 warf eine kleines UAV ein Paket mit radioaktivem Sand auf das Dach des Büros des japanischen Premierministers und protestierte damit gegen die Atomenergiepolitik der japanischen Regierung (Friese, et al., 2016). Expert:innen erwarten eine deutliche Zunahme solcher Bedrohungen (Rassler & Veilleux-Lepage, 2024). Die Möglichkeit der dezentralen Fertigung (3D-Druck) sowie die Möglichkeit, UAVs vor Ort zu produzieren und Reparaturen durchzuführen, können die Verfügbarkeit und Effizienz für böswillige Akteure weiter erhöhen. Ein weiteres Risiko besteht in der Rekombination von UAV mit anderen emergierenden Technologien. Drohnen könnten in Zukunft auch für High-Tech-Innovationen verwendet werden. Technologien wie Gesichtserkennung, LLM/KI, Autonomie/Robotik, Nanosprengstoffe, Energiewaffen, verbesserte Rechenleistung und Data-Mining erhöhen das Potenzial für bislang nicht bekannte Einsatzmöglichkeiten (Rassler, 2016; Rassler & Veilleux-Lepage, 2024).

Anti-Drohnen-Systeme benötigen moderne Erkennungssysteme

Die rasante Entwicklung der Drohnentechnologie macht eine effektive Drohnenabwehr zu einem technologischen Wettlauf. Anti-Drohnen-Systeme benötigen zum einen moderne Erkennungssysteme, die Drohnen rechtzeitig identifizieren können, bevor sie eine Gefahr darstellen. Zum anderen müssen die identifizierten Drohnen anschließend mit geeigneten Methoden unschädlich gemacht werden. Erkennungssysteme stützen sich auf verschiedene Sensoren wie Radar, optische Sensoren, Infrarotsensoren, akustische Detektoren und sogar Radiofrequenzanalyse (Park, et al., 2021). Das Aufspüren kleiner Drohnen stellt besonders hohe Ansprüche an die Sensorik. Millimeterwellen-Radar eignet sich gut für die Erkennung von Kleinstdrohnen auf große Entfernungen.[2] Zur Anwendung kommt auch die Analyse von Frequenzbändern (z. B. Wi-Fi, Bluetooth) oder Funkfrequenzen, die von Drohnen zur Kommunikation genutzt werden. Andere Systeme verarbeiten Videobilder oder Wärmebilder, um bewegende Objekte in der Luft zu erkennen, indem per Software verdächtige Bewegungsmuster erkannt werden können. Detektionssysteme müssen in Echtzeit arbeiten, vornehmlich in Hochsicherheitsumgebungen, um auf Bedrohungen zu reagieren, bevor sie gefährlich werden. Moderne Systeme verwenden KI-gesteuerte Algorithmen, um Bedrohungen schneller zu erkennen und Entscheidungen zu treffen.

[1] *correctiv.org/hybride-kriegsfuehrung/2025/02/18/spionage-drohnen-ueber-deutschland*.
[2] *fhr.fraunhofer.de/de/bereiche/Industrielle-Hochfrequenzsysteme-IHS/kleindrohnendetektion-mit-millimeterwellenradar.html*.

Harte oder weiche, High- oder Low-Tech-Maßnahmen:

- Hochenergielaser

- Netze

- Kamikazedrohnen

- Projektile

- Jamming

- Übernahme der Kommunikation

Bei der Drohnen-Neutralisierung unterscheidet man zwischen *weichen* Maßnahmen, bei denen die Drohne zur Landung gezwungen wird, und *harten* Maßnahmen, bei denen die Drohne physisch abgefangen oder abgeschossen wird. Letztere umfassen sowohl Hightech- als auch Lowtech-Lösungen (Park et al., 2021). Zu den fortschrittlichsten Technologien gehören mit Mikroraketen ausgestattete Anti-Drohnen-Drohnen[3] sowie Directed Energy Weapons (DEWs). Hochenergielaser (HELs) zeichnen sich als besonders kostengünstige Lösung aus, die Drohnen durch fokussierte Strahlenerwärmung zu einem Preis von etwa einem US-Dollar pro Schuss deaktivieren können. Einfachere Abfanglösungen sind Netze, der Einsatz von Kamikazedrohnen und verschiedene projektilbasierte Maßnahmen. Bei den weichen Maßnahmen wurden mehrere ausgeklügelte elektronische Lösungen entwickelt, um unbefugte Drohneneinsätze zu unterbinden. Diese versammeln sich unter dem Stichwort „Jamming". Hochleistungsmikrowellen (HPM), die elektromagnetische Impulse erzeugen, sind speziell darauf ausgelegt, die Elektronik von Drohnen zu stören, und erweisen sich als besonders wirksam gegen koordinierte Drohnenschwarmangriffe. Hochfrequenzstörer (RF) senden gezielt Hochfrequenzenergie aus, um die Kommunikationsverbindungen zwischen Drohnen und ihren Steuerungen zu unterbrechen, während GPS-Spoofing-Technologien falsche Navigationssignale senden, um die Leitsysteme von Drohnen in die Irre zu führen. Am beeindruckendsten ist vielleicht, dass Cyber-Übernahmesysteme entwickelt wurden, die es Behörden ermöglichen, die vollständige Kontrolle über UAVs zu erlangen, indem sie deren Kommunikationsinfrastruktur ins Visier nehmen.

Abwehr nicht-militärischer Drohnen als kommerziell erfolgreicher Markt

Bei der nichtmilitärischen Abwehr von Drohnen werden weiche Maßnahmen gegenüber harten in der Regel bevorzugt, um Kollateralschäden durch abstürzende Drohnen zu vermeiden. Die Frage, welche Systeme am besten geeignet sind, ist nicht zuletzt auch eine Kostenfrage. Militärische Anwendungen von Drohnenabwehrsystemen haben mehrere fortschrittliche Funktionen integriert, die sie für zivile Anwendungen in der Regel zu anspruchsvoll und kostspielig machen. Der kommerzielle Markt für Lösungen zur Drohnenabwehr hat ein bemerkenswertes Wachstum verzeichnet und mehrere Unternehmen, auch aus Österreich, bieten Abwehrsysteme für den zivilen Bereich an. Beim Großen Preis von Österreich der Formel 1 wurde etwa das AARTOS-Drohnenerkennungssystem eingesetzt, um Zuschauer, Fahrer und Crews vor dem illegalen Einsatz von Drohnen zu schützen.[4] Das System, das von einer mobilen Einheit aus bedient wurde, erkannte und kontrollierte erfolgreich nicht autorisierte Drohnen. Zum Schutz der rund 250.000 Zuschauer bei der Airpower24-Flugschau in Zeltweg setzte das Österreichische Bundesheer in Zusammenarbeit mit AARONIA Austria Drohnenabwehrstrategien um.

---

[3] *derstandard.at/adblockwall/story/3000000263216/airbus-stellt-eine-europaeische-anti-drohnen-drohne-mit-mikroraketen-vor?ref=niewidget*.

[4] *drone-detection-system.com/news/austrian-grand-prix-aaronias-high-speed-drone-detection-system-aartos-supports-security-teams-during-formula-1-weekend-in-spielberg/*.

Zu klären sind schwierige rechtliche und organisatorische Fragen

Wie die Sicherheitsbehörden mit der zunehmenden Zahl von unidentifizierten Drohnen unklarer Herkunft über kritischen Infrastrukturen und militärischen Einrichtungen umzugehen haben, ist nicht zuletzt eine schwierige organisatorische und rechtliche Frage. Ob Privatpersonen Drohnen abschießen dürfen, ist nicht eindeutig geregelt und hängt z. B. von der Verletzung von Persönlichkeitsrechten und der Verhältnismäßigkeit der Mittel ab.[5] Das Aufstellen von Störsendern (Jamming) ist hingegen in Österreich nur Sicherheitsbehörden vorbehalten.[6] Die EU-Kommission hat 2023 eine umfassende Strategie zur Abwehr potenzieller Bedrohungen durch zivile Drohnen vorgestellt, mit der sichergestellt werden soll, dass die rasanten technischen Entwicklungen und die wachsende Zahl von Drohnen nicht zu einer unkontrollierten Zunahme der Bedrohungen im zivilen Raum führen.[7] Die konkreten Zuständigkeiten für den Schutz von Einrichtungen und der Bevölkerung sowie der Umgang mit Entscheidungsdilemmata (z. B. Inkaufnahme von Kollateralschäden bei unidentifizierten Drohnen) gilt es national zu regeln.

RELEVANZ DES THEMAS FÜR DAS PARLAMENT UND FÜR ÖSTERREICH

Umgang mit Drohnen im Luftraum durch EU- Recht geregelt – nationale Sonderregelungen sind möglich

Die Anzahl privat und gewerblich genutzter Drohnen nimmt in Österreich stark zu – bis 2023 wurden bereits über 70.000 Drohnenführerscheine ausgestellt.[8] Gemäß der EU-Drohnen-Verordnung können die Mitgliedsstaaten Flugverbotszonen, beispielsweise für Flughäfen oder militärische Einrichtungen, festlegen.[9] Die Verantwortung für die Abwehr und Kontrolle von Drohnen ist in Österreich auf mehrere Regierungsstellen verteilt. Auf operativer Ebene ist die *Austro Control GmbH* die wichtigste untergeordnete Zivilluftfahrtbehörde Österreichs, die für die Sicherheit und Gefahrenabwehr in der Zivilluftfahrt zuständig ist und gleichzeitig Drohnenvorschriften umsetzt. Wenn Vorfälle auftreten, müssen diese zunächst dem Such- und Rettungszentrum von Austro Control gemeldet werden, das diese Meldungen dann an die Sicherheitsuntersuchungsstelle (SUB) weiterleitet. Die SUB, die mit der Untersuchung von Vorfällen im Zusammenhang mit Drohnen betraut ist, bewertet jeden Fall und entscheidet, ob eine vollständige Untersuchung erforderlich ist. Die praktische Umsetzung der Drohnenabwehr, insbesondere in städtischen Gebieten und bei öffentlichen Veranstaltungen, obliegt den Sicherheitsbehörden wie Bundes- oder Landespolizei und zum Teil auch der Direktion für Staatsschutz und Nachrichtendienst (DSN). Unter welchen Bedingungen auch Privatpersonen bzw. -unternehmen Drohnen bekämpfen können (und mit welchen Mitteln), ist rechtlich nicht eindeutig geregelt.

---

5 *wienrecht.at/?view=article&id=430:darf-man-drohnen-abschiessen&catid=15*.
6 *industriemagazin.at/fuehren/industriespionage-ist-die-drohnenabwehr-rechtlich-gedeckt/*.
7 *eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52023DC0659*.
8 *austrocontrol.at/unternehmen/medien/presse__news/detail/austro_control_dronespace_neu_drohnen-verkehrsmanagement_fuer_oesterreich_ist_startklar__1*.
9 *oesterreich.gv.at/themen/reisen_und_freizeit/Drohnen/EU-Regelungen-f%C3%BCr-Drohnen-im-%C3%9Cberblick.html*.

VORSCHLAG WEITERES VORGEHEN

Zum Schutz der Bevölkerung muss die Entwicklung der Drohnentechnologie kontinuierlich beobachtet und bewertet werden

Angesichts der kontinuierlichen Weiterentwicklung von Drohnentechnologie und der Funktionalität für z. T. auch böswillige Zwecke, kommen Organisationen mit Sicherheitsaufgaben nicht umhin, ein permanentes Technologiemonitoring zu organisieren. Zudem müssen organisatorische Zuständigkeiten, Regelungen und Leitlinien für Drohnenerkennung und -abwehr definiert, fortlaufend weiterentwickelt und letztlich auch durchgesetzt werden. Es ist aus heutiger Sicht unklar, welche High- oder Low-Tech-Innovationen durch die Rekombination unterschiedlicher Technologien für die zivile Sicherheit zur Bedrohung werden können. Vor allem die Kreativität zur permanenten Suche nach einem technischen Vorteil in der Kriegsführung, wie aktuell in der Ukraine zu beobachten, erhöht die Wahrscheinlichkeit der baldigen Verfügbarkeit und Einsetzbarkeit unerwünschter Drohnenfunktionalitäten. Eine TA-Studie könnte erheben, welche Missbrauchsrisiken sich durch Fortschritte in der Drohnentechnologie ergeben, und die verfügbaren Abwehrtechnologien mit ihren Vor- und Nachteilen kartieren. Dabei wären auch Kostenaspekte sowie die speziellen Herausforderungen der Situation in Österreich herauszuarbeiten.

ZITIERTE LITERATUR

Del Re, A., et al. (Hrsg.) (2024). *Unbemannte Luftfahrtsysteme: Zivile Drohnen im Spannungsfeld von Wirtschaft, Recht, Sicherheit und gesellschaftlicher Akzeptanz*. Wiesbaden: Springer Fachmedien Wiesbaden. ***doi.org/10.1007/978-3-658-43719-0***.

Friese, L., Jenzen-Jones, N. R., & Smallwood, M. (2016). *Emerging unmanned threats: The use of commercially-available UAVs by armed non-state actors*.

Lonstein, W. D. (2020). *C-UAS Regulation, Legislation, & Litigation from a Global Perspective*. ***kstatelibraries.pressbooks.pub/counterunmannedaircraft/chapter/chapter-12-global-perspective-whats-legal-where-trends-gaps-covers-discuss-chinese-iranian-and-russian-c-uas-lonstein/***.

Park, S., et al. (2021). Survey on Anti-Drone Systems: Components, Designs, and Challenges. *IEEE Access*, *9*, 42635–59. ***doi.org/10.1109/ACCESS.2021.3065926***.

Rassler, D. (2016). *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology*. West Point: Combating Terrorism Center. ***govinfo.gov/content/pkg/GOVPUB-D109-PURL-gpo182659/pdf/GOVPUB-D109-PURL-gpo182659.pdf***.

Rassler, D., & Veilleux-Lepage, Y. (2024). The paradox of progress: How 'disruptive,' 'dual-use,' 'democratized,' and 'diffused' technologies shape terrorist innovation. *TATuP – Journal for Technology Assessment in Theory and Practice*, *33*(2), 22–28. ***doi.org/10.14512/tatup.33.2.22***.