Herausforderung Drohnenmissbrauch – ein neues Spannungsfeld für Safety und Security

Abusive Operation of Drones – A New Challenge for Safety and Security

Julia Gonschorek, Rico Kelz

European Aviation Security Center e. V., Trebbin/Schönhagen · gonschorek@easc-ev.org

Zusammenfassung: Die steigende Zahl der unerlaubten Drohnenflüge stellen Sicherheitskräfte vor neue Herausforderungen. Täter sind häufig Personen, die uninformiert/ignorant Luftfahrzeuge aufsteigen lassen. Den Missbrauch zu verhindern oder schadensfrei abzuwenden und die Tat zu ahnden, fällt schwer: eine Registrierungspflicht fehlt, Detektionstechnologien sind unausgereift, Abwehrtechnologien gänzlich verboten. GIS für die Flugroutenplanung und Geofencing sind erste Schritte, um fahrlässiges Handeln einzudämmen. Kriminelle Handlungen bleiben in geoinformatischen Ansätzen unberücksichtigt. In diesem Spannungsfeld sind die BMBF-Projekte MIDRAS und ArGUS eingebettet, deren bisherige Forschungsergebnisse Gegenstand des Artikels sind.

Schlüsselwörter: Drohne (UAS/UAV/RPAS/CPS), Abwehr, GIS, zivile Sicherheit

Abstract: *The increasing number of this kind of cyber-physical systems defines a completely new, and unexpected for a decade ago, challenges for civil safety and security tasks. In civil context a lack of knowledge is the most common reason of abusive operated drones. It's amitous to prevent, or to avoid it without any damage, and to assert the applicable law: there is no registration requirement, technologies to detect are not that fail-safe, and C-UAS is not allowed in general. Using GIS for flight planning and geofencing are first steps for a safe integration of drones into airspace. Criminal, intentional, actions remain problematic. Subject of this article are preliminary results of the BMBF-Projects MIDRAS and ArGUS, integrated into this challenging field.*

Keywords: *Drone (UAS/UAV/RPAS/CPS), Counter-UAS, GIS, Civil Safety & Security*

1 Das Spannungsfeld: Drohnenintegration in den Luftraum

Drohne ist eine politisch akzeptierte Sammelvokabel für unbemannte Luftfahrtsysteme und wird häufig synonym für Unmanned Aerial/Aircraft Vehicle (*UAV*), Unmanned Aerial/Aircraft System (*UAS*), Remotely Piloted Aircraft Systems (*RPAS*) oder auch Cyber-Physische Systeme (*CPS*) verwendet. Bei UAV handelt es sich ausschließlich um das unbemannte Fluggerät, während UAS, RPAS und CPS tatsächlich das gesamte Flugsystem inklusive aller Ladungen (*engl.: payload*) umfasst. RPAS können als eine besondere Untergruppierung von UAS klassifiziert werden: hierbei handelt es sich um ferngesteuerte oder vollautomatisch betriebene Systeme (vgl. European Commission, 2014).

Entwicklungsgeschichtlich betrachtet, sind Drohnen eine relativ junge Militärtechnologie: ursprünglich ein Spähwerkzeug für die strategische Kriegsführung und gegenwärtig zunehmend als Waffe gegen den Feind im Krieg aus der Ferne. In den vergangenen Jahren war eine sprunghafte Kommerzialisierung und Diffusion dieser Technologie in die Wirtschaft und Privathaushalte zu beobachten. Allein in 2016 wurden die Verkaufszahlen (weltweit)

AGIT – Journal für Angewandte Geoinformatik, 4-2018, S. 356-364. © Wichmann Verlag, VDE VERLAG GMBH · Berlin · Offenbach. ISBN 978-3-87907-647-5, ISSN 2364-9283, eISSN 2509-713X, doi:10.14627/537647045.

zivil genutzter Drohnen auf circa 2.425.000 geschätzt (Statista, 2016). Die Deutsche Flugsicherung geht davon aus, dass im vergangenen Jahr 600.000 solcher unbemannten Luftfahrzeuge in Deutschland verkauft wurden (DFS Deutsche Flugsicherung GmbH & Deutsche Telekom AG, 2017).

Ferner ist festzuhalten, dass *Drohne* nicht einen einzigen Typus meint, sondern vielmehr von einer enormen Vielfalt auszugehen ist: Starrflügler und Multirotorsysteme bzw. Multikopter und Hybridsysteme – also Starrflügler, die in der Lage sind, vertikal zu starten und zu landen (*VTOL*). Eine weitere Ausdifferenzierung ist über die enorme Heterogenität hinsichtlich Flugdauer, -höhe, -geschwindigkeit, Traglast und nicht zuletzt ihrer Nutzungsart gegeben. Die EU vergleicht die gesellschaftliche Tragweite dieser Technologie mit der Alltagsbeeinflussung durch das Internet seit den 1990er-Jahren (European Commission, 2014). In der EU-Strategie *Flightpath 2050* werden Vorzüge von Drohnen nicht nur innerhalb des Luftfracht-Sektors identifiziert: „These include new applications, for example providing part of society's information infrastructure, a variety of monitoring functions, disaster relief, etc. Rotorcraft play a significant role in public services, including search and rescue, and also in (regional) transport" (European Commission, 2011, p. 10). Von zentraler wirtschaftlicher Bedeutung ist künftig auch der Grad der Automatisierung und Flug außerhalb der Sichtweite (vgl. Karpowicz, 2018). Während die Europäische Kommission 2014 noch davon sprach, „Maßnahmen zu ergreifen, um eine schrittweise Integration von RPAS in den zivil genutzten Luftraum ab 2016 zu ermöglichen" (European Commission 2014, p. 2), ist ein regelrechter Boom an kommerziell genutzten Drohnen in Deutschland seit etwa drei Jahren zu beobachten. In 2016 meldete die DFS insgesamt 61 Störungen des Luftverkehrs durch Drohnen (DFS Deutsche Flugsicherung GmbH). Nicht nur Flughäfen sehen sich vor neue Herausforderungen an ihr Sicherheitskonzept gestellt. Zäune werden mit diesen vergleichsweise einfachen und kostengünstigen Mitteln ad absurdum geführt. Hierfür braucht es lediglich eine Drohne mit Sensorik (z. B. Kamera) und ein Smartphone mit Internetverbindung. Missbrauch erhält durch diese Technologie eine völlig neue Dimension. Dabei spielt die Drohne an sich – im wahrsten Sinne – eine tragende Rolle. Sie ist in der Lage, Ladung mitzuführen. Das Möglichkeitsspektrum für die zivile Sicherheit gefährdende Handlungen ist groß und umfasst Rechtswidrigkeiten von Verletzung der Privatsphäre über Industriespionage bis hin zu Anschlägen mit Homemade-Explosives.

Eingriffe in die Privatsphäre, Spionage und weitere kriminelle sowie terroristische (Vorbereitungs-)Handlungen stellen nicht nur mögliche Szenarien, sondern bereits eingetretene Gefahrenlagen dar. Ein Versuch auf nationaler Ebene, die Kontrolle zurückzuerlangen, ist die im Frühjahr 2017 in Kraft getretene Drohnenverordnung. Die sichere Integration von Drohnen in den Luftraum ist das erklärte Ziel auf nationaler, EU- und internationaler Ebene. „RPAS sind nicht vor illegalen Tätigkeiten sicher […]. Die für die Verwaltung der 4D-Flugwegdaten im künftigen Flugverkehrsmanagementsystem und die Fernsteuerung von Luftfahrzeugen erforderlichen Informationen werden von verschiedenen Luftfahrtbetreibern in Echtzeit übermittelt und geteilt werden müssen, um die Leistung des Systems zu optimieren […]. Aus den festgestellten Sicherheitserfordernissen werden anschließend unter Aufsicht der zuständigen Behörden rechtliche Verpflichtungen für alle relevanten Akteure wie Navigationsdienstleister, RPAS-Betreiber oder Telekommunikationsdienstleister abgeleitet […], Die Kommission stellt sicher, dass sich die Vorschriften für den RPAS-Betrieb auch auf den Schutz vor unrechtmäßigen Eingriffen erstrecken, so dass die Hersteller und die Betreiber geeignete Maßnahmen zur Gefahrenminderung ergreifen können" (European Commission, 2014, p. 8). Als einen Pfeiler dieser Strategie fördert das Bundesministerium für Bildung und

Forschung im Rahmen der Bekanntmachung „Aspekte und Maßnahmen der Terrorismusbekämpfung“ des Sicherheitsforschungsprogrammes seit 2017 insgesamt vier FuE-Kooperationsprojekte mit den Forschungsschwerpunkten Drohnenmissbrauch, -detektion und -abwehr. Erste EASC-Forschungsergebnisse aus zwei Projekten werden hier vorgestellt. Im Projekt MIDRAS (Mikro-Drohnen-Abwehr-System) werden bestehende Drohnenabwehr-Technologien um innovative Techniken erweitert. Das modulare System soll sowohl Detektion und Klassifikation von Drohnen als auch den Einsatz aktiver Abwehrtechnologien ermöglichen. Der Fokus des EASC liegt auf der detaillierten Modellierung von Gefahrenszenarien und der rechtlichen Begleitforschung. In ArGUS (Assistenzsystem zur situationsbewussten Abwehr von Gefahren durch Drohnen) entwickelt das Konsortium ein Einsatzassistenzsystem, das Drohnen durch kombinierte Sensorik frühzeitig erkennen und Einsatzkräften eine detaillierte Bedrohungsanalyse sowie gegebenenfalls zielgruppenspezifische Handlungsempfehlungen geben kann. Das EASC evaluiert hier die Schulungsbedarfe des Sicherheitspersonals, entwickelt Lehrinhalte und erarbeitet Sensibilisierungskonzepte für die Zivilbevölkerung.

2 Drohnenmissbrauch im Kontext von Safety & Security

2.1 Differenzierung des Sicherheitsbegriffs

Die Gewährleistung der zivilen Sicherheit – ein Grundpfeiler unserer Demokratie und Rechtsstaatlichkeit – ist zunächst einmal Aufgabe des Staates. Dabei bilden zuverlässig funktionierende Infrastrukturen (z. B. Kommunikation, Ver- und Entsorgung, Verkehr) das Fundament unserer Gesellschaft. „Sicherheit ist ein komplexer Relationsbegriff, in dem das Risiko eines Systems mit einem unvertretbaren Risiko verglichen wird, welches einen oberen Grenzwert darstellt. Der zur „Sicherheit“ komplementäre Begriff ist der Begriff der Gefahr. Die „Gefahr“ ist definiert als Sachlage, bei der das Risiko größer als das vertretbare Risiko. Um das „Risiko“ zu erklären, bedarf es des Begriffs des Schadens, der als Umfang oder Ausmaß der Schädigung der Gesundheit von Menschen, von Gütern oder der Umwelt definiert ist“ (Schnieder & Schnieder, 2010, pp. 102 f.). Sicherheit wird in der Wissenschaft und Wirtschaft differenziert in Safety und Security. Safety ist gleichbedeutend mit dem Schutz vor ungewollten bzw. fahrlässigen oder zufälligen Systemauswirkungen, wohingegen Security den Schutz des Systems vor vorsätzlichem Handeln, also einer gewollten Gefährdung durch Fremdeinwirkung zum Zwecke der Schädigung oder Bereicherung, umfasst (vgl. Beyerer et al., 2010; Schnieder & Schnieder, 2010). Diese begriffliche Grenze verschwimmt jedoch, wenn der Fokus auf das Schutzziel (Mensch und Gut) gerichtet wird. Unabhängig von Fahrlässigkeit oder Vorsatz muss das Sicherheitspersonal befähigt sein, Gefahren zu erkennen und im Idealfall abzuwenden, das Schadensausmaß zu reduzieren und Täter zu identifizieren.

2.2 Drohnenmissbrauch

Der Terminus *Drohnenmissbrauch* hat bislang keinen Eingang in die Rechtsprechung gefunden. Hinsichtlich der Safety- und Security-Charakteristika solcher Handlungen, setzen ArGUS und MIDRAS folgende Arbeitsdefinition:

Die missbräuchliche Nutzung von Drohnen wird differenziert in unabsichtlich (fahrlässig; Safety-relevant) und absichtlich (vorsätzlich; Security-relevant). Der ***unabsichtliche Missbrauch*** *versteht sich als Handlung des Drohnenpiloten, die auf Uninformiertheit basiert und*

der Rechtsprechung entgegensteht. Dieses Handeln kann zu Personen-, Sach-, finanziellem oder ideellem Schaden führen. Der ***absichtliche Missbrauch*** *umfasst die Androhung und Durchführung einer vorsätzlich schadhaften oder bereichernden Handlung durch den Drohnenpiloten (und möglicherweise dessen Auftraggeber). Täter sind Privatpersonen mit persönlichem Motiv, organisierte Kriminelle und Terroristen bzw. terroristische Netzwerke. Dieses Handeln soll zu Personen-, Sach-, finanziellem oder ideellem Schaden führen.*

Hiernach können Missbrauchsarten klassifiziert und deren mögliche Konsequenzen abgebildet werden (vgl. Kapitel 2.3). Jede Klasse birgt Risiken in teils unterschiedlichen Ausprägungen und Schweregraden. Dies umfasst u. U. Schadenslagen beispielsweise durch:

- die Drohne oder den Drohnenschwarm (physisch durch Fluggeschwindigkeit, Gewicht, Rotorblätter, Batterie etc. bei Absturz oder Kollision),
- die intern/extern angebrachte Ladung der Drohne (z. B. giftige, explosive Gefahrenstoffe),
- die Sensorik an der Drohne (z. B. optisch, akustisch).

Die Bundesstelle für Flugunfalluntersuchungen veröffentlich regelmäßig Unfall- und Sichtungsstatistiken. Auch die DFS Deutsche Flugsicherung hält Sichtungen und Vorfälle fest. Die Luftfahrtbehörden der Länder führen Listen über Ordnungswidrigkeiten und Straftaten leiten diese im Rahmen der bundesweiten Meldeverfahren zu Sachverhalten mit sicherheitsrelevantem Bezug an die Informationssammelstelle für unbemannte Luftfahrzeuge (*KOST Drohne*) weiter. Diese Daten sind nur auf Anfrage erhältlich und i. d. R. ohne Geokoordinaten und relevante Metainformationen wie z. B. Wetterbedingungen. Damit sind repräsentative Geovisualisierungen und Analysen gegenwärtig nicht möglich. Festzuhalten ist jedoch die bedenkliche Entwicklung: Die Zahl der offiziell gemeldeten Vorfälle steigt seit 2015 in Deutschland jährlich rasant an (monatsgenau vgl. z. B. Bundesstelle für Flugunfalluntersuchung, 2017).

Da die Folgen missbräuchlichen Handelns für das Sicherheitspersonal i. d. R. nicht frühzeitig erkennbar sind, „the security practitioner should focus on developing and implementing practical systems, measures, and procedures to prevent all forms of attack and criminal activity“ (Price & Forrest, 2013, pp. xix f.). Im Rahmen der in ArGUS durchgeführten 26 Expertengespräche und Befragungen, sehen Behörden und Organisationen mit Sicherheitsaufgaben (*BOS*), private Sicherheitsdienstleister und Verbände gegenwärtig die Safety-relevanten Folgen von fahrlässigen Handlungen als größtes Problem, gefolgt von kriminellem und terroristischem Handeln. In der Sicherheitsforschung setzen sich zunehmend szenarienorientierte Forschungsansätze durch. „[Dies] […] soll zu systematischen, sicherheitsrelevanten Gesamtkonzepten führen und, basierend auf Risikoanalysen, die Angreifbarkeit und Verwundbarkeit der betrachteten Systeme minimieren“ (Thoma, Drees & Leismann, 2010, p. 14). In MIDRAS und ArGUS werden ebensolche Szenarien modelliert und mit den Bedarfsträgern evaluiert. Hierzu zählt neben der Entwicklung und Implementierung von Technologien vor allem die Sensibilisierung des Sicherheitspersonals für die Gefahrenpotenziale. Daneben gilt es, das Personal zu schulen. Stichworte sind hier: Achtsamkeit/Aufmerksamkeit, Definition von Handlungsreihenfolgen und Einsatzketten, Kenntnis der Rechtsgrundlagen sowie die Bedienung der Technologie(n).

2.3 Drohnenmissbrauch im Bereich von Justizvollzugsanstalten: Identifikation von Gefährdungsszenarien

„Generell geht der Verordnungsgeber bei Geräten bis 250 Gramm von keinem erhöhten Risiko für Personen am Boden und den bemannten Luftverkehr aus, im Bereich von 0,25 kg bis 5 kg lediglich von einem erhöhten Risiko für Personen am Boden und im Bereich von 5 kg bis 25 kg von einem erhöhten Risiko für beide Gruppen“ (Beck 2017, p. 124). Dass diese Sichtweise perspektivisch nicht tragfähig ist, belegen eingangs benannte Statistiken und Berichte über teils schwere Störungen durch Drohnen, für deren Betrieb noch kein Kenntnisnachweis erforderlich ist. Ein besonderer Fokus liegt auf dem Schutz kritischer Infrastrukturen. „Safety-critical systems are those systems whose failure could result in loss of life, significant property damage or damage to the environment. Many modern information systems are becoming safety-critical“ (Knight, 2002, p. 547). Zu diesen Strukturen zählen auch Justizvollzugsanstalten (*JVA*). Gefährdungsszenarien und die mit deren Eintreten verbundenen Gesetzes- und Verordnungsverstöße werden in Abbildung 1 zusammenfassend dargestellt. Bei den Verstößen wird zwischen Ordnungswidrigkeit und Straftat unterschieden. In Deutschland sind Ordnungswidrigkeiten jedoch lediglich geringfügigere Gesetzesübertretungen, die (noch) nicht den Unrechts-Charakter einer Straftat erfüllen.

Die JVA-Szenarien befassen sich im Bereich ***Safety*** mit den ***Missbrauchsklassen***:

- ***Überflug*** mit einer Drohne und dem Eindringen in eine Flugverbotszone mit einer Drohne. Dabei kommt es zu einer Zuwiderhandlung gegen Luftsperrgebiete und Flugbeschränkungen, sowie zum generell verbotenen Betrieb von unbemannten Luftfahrzeugen.
- Anfertigung von ***Fotos/Videos*** mit einer Drohne von einer JVA, bzw. von deren Insassen und Bediensteten, sowie die ***Veröffentlichung*** dieser Daten.

Und im Bereich ***Security*** mit den ***Missbrauchsklassen***:

- Flugmanövern mit einer Drohne zur ***Ablenkung*** des JVA Personals. Die Drohne kann genutzt werden um von Straftaten respektive Ordnungswidrigkeiten in der JVA einzuleiten oder zur Ablenkung vom eigentlichen Vergehen.
- ***Angriff*** mit einer Drohne. Dabei ist die Drohne zum Beispiel mit Sprengstoff, Schusswaffen oder informationstechnischen Vorrichtungen ausgerüstet. Es können Justizbeamte, Polizeibeamte, Insassen bzw. andere Bedienstete der JVA verletzt oder getötet werden. Des Weiteren können Sachbeschädigungen, durch z. B. Brand- und Sprengsätze, oder ***Sabotage***, durch z. B. Datenveränderung und Computersabotage, mithilfe von Informationstechnischen Vorrichtungen herbeigeführt werden.
- Anfertigung von ***Fotos/Videos*** mit einer Drohne von einer JVA, bzw. von deren Insassen und Bediensteten, sowie die ***Veröffentlichung*** dieser Daten, mithilfe derer Sicherheitsabläufe und die Sicherheitsinfrastruktur der JVA ausgespäht und für weitere Aktionen genutzt werden (***Spionage***).
- ***Einbringung*** von Gegenständen, wie z. B. Drogen, Mobiltelefon, Waffen, Nachrichten und Informationen in die JVA unter der Verwendung einer Drohne.

Die Identifikation und weitere Ausdifferenzierung dieser Szenarien ist ein erster Schritt, um Gefahrenpotenziale zu ermitteln und Strategien zum Umgang mit diesen Herausforderungen zu entwickeln.

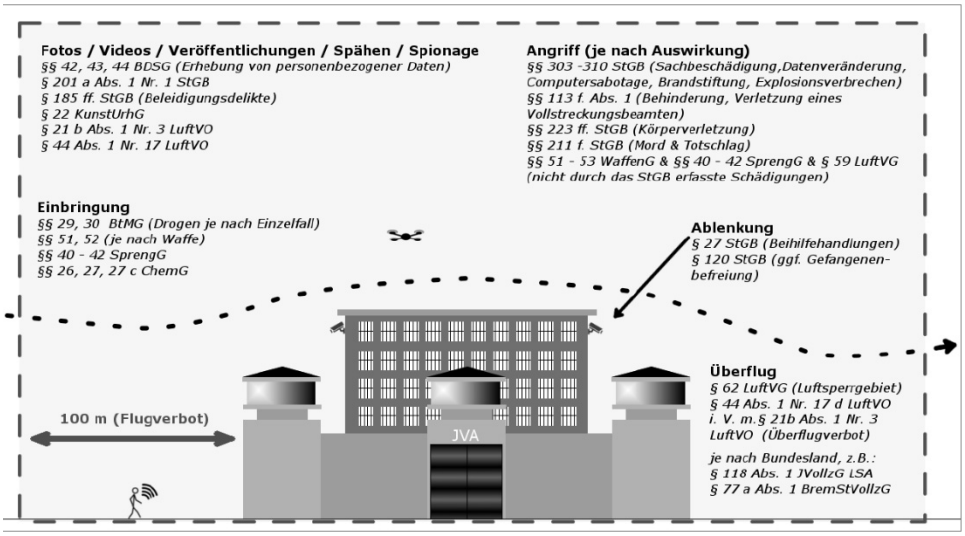

Abb. 1: Übersicht über Gefährdungen durch Drohnenmissbrauch im JVA-Szenario

3 Sichtbarkeit und Prävention: Beitrag von GIS zur Erhöhung der Safety

In Deutschland gibt es gegenwärtig keine verpflichtende Registrierung von Drohnen und keine flächendeckenden Detektionssysteme. In der Folge gibt es auch kein einheitliches, amtliches Flugverkehrsmanagementsystem, das auch Drohnenflüge integriert. Aktive Abwehrmaßnahmen sind im zivilen Bereich gänzlich verboten. International befasse sich zahlreiche Unternehmen bzw. Initiativen mit dem Thema aktiver Drohnenabwehr (vgl. Butterworth-Hayes, 2018).

Geofencing wird oftmals herstellerseitig genutzt, um unerlaubtes Eindringen von Drohnen zu verhindern. Beim Überschreiten einer virtuell definierten Begrenzung auf der Erdoberfläche oder im Luftraum wird ein Automatismus in der Drohne ausgelöst. So können Flugverbotszonen (*engl.: No-Fly-Zone; NFZ*) softwaresystemisch erzeugt werden, aus denen heraus die Drohne nicht starten können bzw. am Einflug gehindert wird (vgl. Gärtner, 2011). Kontrollzonen von Flugplätzen, Krankenhäusern, über Gebäuden von Verfassungsorganen, Bundes- und Landesbehörden, Industrieanlagen, Wohngrundstücken, Naturschutzgebieten, Menschenansammlungen und den Einsatzorten von Polizei und Rettungskräften sind gemäß Drohnenverordnung Flugverbotszonen. Diese NFZ werden von einigen Herstellern in deren Drohnensoftware implementiert.

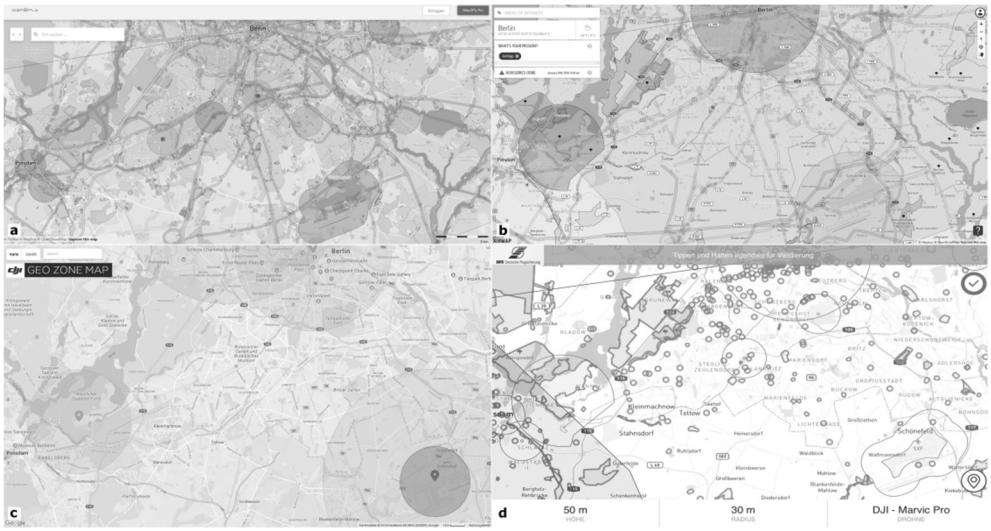

Abb. 2: Software-Applikationen zur Flugroutenplanung der Anbieter: a) FlyNex Map2Fly, b) Airmap, c) DJI geo zone map und d) Unifly & DFS Deutsche Flugsicherung (Bildquellen: a) FlyNex, b) Airmap, c) DJI, d) Unifly/DFS 2018)

Safety-relevant sind ebenfalls GIS-Softwares, -Applikationen und Web-Map-Services, die die Flugroutenplanung unterstützen, indem flugrelevante Informationen sichtbar gemacht werden. Hierzu zählen typen-offene Systeme und typ-gebundene Systeme (Angebote der Drohnenhersteller). Abbildung 2 zeigt eine Auswahl grafischer Benutzeroberflächen dieser Anwendungen. Noch sind die Laufendhaltung, Vollständigkeit und korrekte Objekt-Zeichen-Referenzierung, z. B. als NFZ, der Geodaten problematisch. Die Geodaten stammen aus unterschiedlichen Quellen, teilweise beziehen sich einzelne Systemanbieter auf andere Dienstleister, sodass sich Fehler fortpflanzen. Genutzt werden z. B. OSM-Daten, Google-Maps-Daten, Daten von Lufthansa Technik Lido u. a. Die GIS zeigen mehr oder weniger signifikante Schwachstellen, die im Falle eines dennoch eintretenden Rechtsverstoßes auch zu Haftungsfragen führen können. Hinzu kommt, dass es ein Flugverbot im 100-m-Bereich von Einsatzorten der BOS gibt. Diese sind temporär, die Daten werden in den Einsatzleitstellen der Länder vorgehalten und sind somit noch nicht Bestandteil der Flugroutenplanungs-Anwendungen. Die hierfür notwendige Dateninfrastruktur ist noch zu schaffen.

4 Diskussion

Für die sichere Integration von Drohnen in den zivilen Luftraum bedarf es eines Flugverkehrsmanagementsystems, das bemannte und unbemannte Luftfahrtzeuge integriert, sowie einer zentralen Störungs- und Unfalldatenbank mit hochauflösenden Raum- und Zeitdaten. Eine Grundlage hierfür kann die generelle Registrierungs- und Transponderpflicht sein.

Die stetige Weiterentwicklung und Datenpflege der Anwendungen für die Flugroutenplanung und Informationsintegration in das Flugsystem können in diesem Gefüge einen zunehmend stärkeren Beitrag zur Safety leisten. Künftig gilt es Normen und Standards für diese

Form von GIS zu entwickeln, um eine intuitive sowie sichere Bedienung für Privatpersonen und Gewerbetreibende ohne Tiefenkenntnis in den Bereichen Avionik und Kartographie zu gewährleisten. Eine Flugroutenplanung über standardisierte und zertifizierte Systeme ist als Präventivmaßnahme aufzufassen und sollte perspektivisch Eingang in die nationale Gesetzgebung finden.

Im Bereich der Security stellen missbräuchlich eingesetzte Drohnen ein ernst zu nehmendes Problem dar. Am Beispiel der JVA wurden realistische Gefahrenpotenziale aufgezeigt. Wenn die Drohne gesichtet wird, haben die Sicherheitskräfte nur sehr wenig Reaktionszeit für etwaige Abwehrmaßnahmen, wobei aktive Systeme hierbei i. d. R. nicht zugelassen sind.

Perspektivisch ist festzuhalten, dass geoinformatorische Methoden und Systeme mittelfristig eine tragende Rolle in Prozessen der Personen-, Veranstaltungs- und Objektsicherung gegen Drohnenmissbrauch einnehmen werden.

Literatur

Airmap Inc.: *Airmap*. Retrieved January 31, 2018, from https://app.airmap.io/.

Beck, M. (2017). *Dr. Drohne: Die Drohnen-Verordnung: Bewertung geplanter Normen zur Regulierung ziviler Drohnen anhand von ökonomischen Interessen und gesellschaftlichen Risiken.* Norderstedt: Books on Demand.

Beyerer, J., Geisler, J., Dahlem, A., & Winzer, P. (2010), Sicherheit: Systemanalyse und -design. In: P. Winzer, E. Schnieder, & F.-W. Bach (Eds.), *Sicherheitsforschung: Chancen und Perspektiven (acatech DISKUTIERT)* (pp. 39–72). Berlin: Springer.

Bundesstelle für Flugunfalluntersuchung (2017). *Studie über Annäherungen und Kollisionen von Luftfahrzeugen im deutschen Luftraum 2010-2015.* Retrieved October 17, 2017, from https://www.bfu-web.de/DE/Publikationen/Statistiken/Tabellen-Studien/Tab2017/Studie_AIRPROX_2017.pdf?__blob=publicationFile.

Butterworth-Hayes, P. (2018). *The counter UAS directory: The information portal for unmanned air system traffic management (UTM) and counter-UAS (C-UAS) systems.* Unmanned Airspace, Hove, UK, Retrieved January 22, 2018, from http://www.unmannedairspace.info/wp-content/uploads/2018/01/Counter-UAS-directory-January-2018.pdf.

DJI: *Geo Zone Map.* Retrieved January 31, 2018, from https://www.dji.com/flysafe/geo-map.

DFS – Deutsche Flugsicherung GmbH. *Drohnen Infografiken.* Retrieved October 31, 2017 from https://www.dfs.de/dfs_homepage/de/Presse/Pressemitteilungen/2016/15.11.2016.-%20DFS%20bringt%20bemannte%20und%20unbemannte%20Luftfahrt%20zusammen/drohnen_infografiken.pdf.

DFS – Deutsche Flugsicherung GmbH & Deutsche Telekom AG (2017). *Deutsche Flugsicherung und Deutsche Telekom machen sich für Drohnen-Sicherheit stark: Drone Detection Day informiert über Erkennung und Abwehr Magenta Schutzschild der Öffentlichkeit vorgestellt – DFS und Telekom fordern Registrierungspflicht für Drohnen.* Retrieved January 19, 2018 from

https://www.dfs.de/dfs_homepage/de/Presse/Pressemitteilungen/2017/05.07.2017.-%20Deutsche%20Flugsicherung%20und%20Deutsche%20Telekom%20machen%20sich%20f%C3%BCr%20Drohnen-Sicherheit%20stark/.

European Commission (2011). *Flightpath 2050: Europe's vision for aviation; maintaining global leadership and serving society's needs; report of the High-Level Group on Aviation Research.* Report of the High Level Group on Aviation Research, Publ. Off. of the Europ. Union, Luxembourg. Retrieved January 19, 2018 from https://ec.europa.eu/transport/sites/transport/files/modes/air/doc/flightpath2050.pdf.

European Commission (2014). *Ein neues Zeitalter der Luftfahrt: Öffnung des Luftverkehrsmarktes für eine sichere und nachhaltige zivile Nutzung pilotenferngesteuerter Luftfahrtsysteme.* Mitteilung der Kommission an das Europäische Parlament und den Rat, COM (2014), Brussels.
Retrieved January 19, 2018 from http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52014DC0207&from=EN.

FlyNex: *Map2Fly*. Retrieved January 31, 2018 from https://map2fly.flynex.de/.

Gärtner, S. (2011). Geofencing und Datenschutz: Big Mother is watching you. *Legal Tribune online,* 16. November 2011. Retrieved January 31, 2018, from https://www.lto.de/recht/hintergruende/h/geofencing-und-datenschutz-big-mother-is-watching-you/.

Karpowicz, J. (2018). *8 Commercial Drone Predictions for 2018.* Commercial UAV NEWS. Retrieved January 23, 2018, from https://www.expouav.com/wp-content/uploads/2017/12/8-Commercial-Drone-Predictions-for-2018.pdf.

Knight, J. C. (2002). Safety Critical Systems: Challenges and Directions. *Proceedings of the 24th International Conference on Software Engineering,* May 19 – 25, 2002 (pp. 547–550).

Price, J. C., & Forrest, J. S. (2013). *Practical aviation security: Predicting and preventing future threats.* 2nd Ed. Amsterdam: Elsevier.

Schnieder, E., & Schnieder, L. (2010). Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung. In: P. Winzer, E. Schnieder, & F.-W. Bach (Eds.), *Sicherheitsforschung: Chancen und Perspektiven* (*acatech DISKUTIERT*) (pp. 73–115). Berlin/Heidelberg: Springer.

Springer, M. (2016). *Was ist der Unterschied zwischen Safety und Security?* Projekt Security4Safety, Retrieved January 27, 2018, from https://www.tuev-nord.de/explore/de/erklaert/was-ist-der-unterschied-zwischen-safety-und-security/.

Statista (2016). *Anzahl der verkauften kommerziellen Drohnen weltweit in den Jahren 2013 bis 2017*, Retrieved November 3, 2017, from https://de.statista.com/statistik/daten/studie/660240/umfrage/anzahl-der-verkauften-kommerziellen-drohnen-weltweit/.

Thoma, K., Drees, B., & Leismann, T. (2010). Zukunftstechnologien in der Sicherheitsforschung. In: P. Winzer, E. Schnieder, & F.-W. Bach (Eds.), *Sicherheitsforschung: Chancen und Perspektiven* (*acatech DISKUTIERT*) (pp. 13–37), Berlin/Heidelberg: Springer.

UniFly: *DFS Drohnen App*. Retrieved January 31, 2018.