

Bachelor-Thesis
im Studiengang
Allgemeine Informatik

**Bedrohung von oben:
Analyse des Gefahrenpotenzials von frei
erhältlichen Drohnen für die
Informationssicherheit
von Unternehmen**

Erstgutachter: Prof. Dr. Richard Zahoransky

Zweitgutachter: Dr. Konrad Meier

Vorgelegt am: 22.12.2023

Vorgelegt von: Ben Lutz

266156

██████████

██████████████████

ben.lutz@hs-furtwangen.de

██████████████████

Vorwort

Gender-Hinweis

Die in dieser Arbeit verwendeten Personenbezeichnungen, beziehen sich immer gleichermaßen auf weibliche, männliche und diverse Personen. Zugunsten einer besseren Lesbarkeit werden auf Doppelnennungen und gegenderte Bezeichnungen verzichtet.

Format

Zur Verbesserung der Leserlichkeit weicht diese Arbeit von den formalen Vorgaben der Hochschule Furtwangen ab. Insbesondere wurde die Schriftgröße angepasst. Außerdem wurden Abbildungs-, Tabellen- und Abkürzungsverzeichnis ans Ende der Arbeit verschoben.

Annahme zum 20. Deutschen IT-Sicherheitskongress

Diese studentische Arbeit wurde vom Beirat für das Programm des 20. Deutschen IT-Sicherheitskongresses des Bundesamts für Sicherheit in der Informationstechnik ausgewählt.

Danksagung

An dieser Stelle möchte ich meine Dankbarkeit all jenen aussprechen, die mich während der Erstellung meiner Bachelorarbeit unterstützt und begleitet haben.

Ein herzlicher Dank geht an Herrn Prof. Dr. Richard Zahoransky, mein Betreuer, welcher mit wertvollen Anregungen, Vermittlung von Interviewpartnern und der Zurverfügungstellung von Drohnenhardware maßgeblich zum Gelingen dieser Arbeit beigetragen hat.

Ein besonderer Dank gebührt auch Herrn Dr. Konrad Meier. Sein akademischer, struktureller und fachlicher Rat waren ebenfalls, besonders in herausfordernden Zeiten dieser Arbeit, ein maßgeblicher Faktor für das Gelingen. Ich bedanke mich herzlichst für seinen stets engagierten und intensiven Einsatz bei Anliegen meinerseits.

Zusätzlich danke ich besonders den Interviewpartnern, welche die Ergebnisse dieser Arbeit durch ihre vielschichtigen Meinungen bereichert haben.

Außerdem danke ich allen Beteiligten, die sich Zeit für die Korrektur dieser Arbeit genommen haben.

Abschließend möchte ich meinen Eltern meinen tiefsten Dank aussprechen. Ihre bedingungslose Unterstützung und ihr Glaube an mich während meines gesamten Studiums waren eine ständige Quelle der Inspiration und Stärke.

Abstract

English

This bachelor's thesis comprehensively examines the threat posed by the use of commercially available drones to compromise the information security of organizations. Through a combination of literature analysis, expert interviews, and a case study, this research provides a detailed insight into the diversity of threats and the feasibility of drone supported attacks on information security. It is found that drones present a real and multifaceted threat. Assessing the likelihood of such attacks is complex due to the dynamic development of drone technology and the variety of potential applications. The thesis empathizes the necessity for organizations to develop effective defensive strategies and highlights the importance of further research in this field to meet the challenges of technological advancements and the constantly evolving threat landscape.

Deutsch

In dieser Bachelorarbeit wird die Bedrohungslage durch den Einsatz von frei erhältlichen Drohnen zur Beeinträchtigung der Informationssicherheit von Organisationen umfassend untersucht. Unter Verwendung einer Kombination aus Literaturanalyse, Experteninterviews und Fallstudie wird die Vielfalt der Bedrohungen und die Machbarkeit von Drohnenunterstützte Angriffen auf die Informationssicherheit detailliert beleuchtet. Dabei zeigt sich, dass Drohnen eine reale und vielschichtige Gefahr darstellen. Die Einschätzung der Eintrittswahrscheinlichkeit solcher Angriffe ist aufgrund der dynamischen Entwicklung der Drohnentechnologie und der Vielfalt der Anwendungsmöglichkeiten komplex. Diese Arbeit betont die Notwendigkeit für Organisationen, effektive Abwehrstrategien zu entwickeln, und weist auf die Wichtigkeit weiterer Forschung in diesem Bereich hin, um den Herausforderungen der technologischen Entwicklungen und der sich ständig ändernden Bedrohungslandschaft gerecht zu werden.

Inhaltsverzeichnis

Vorwort	I
Abstract	III
Inhaltsverzeichnis	V
1 Einleitung	1
1.1 Forschungsfrage und Ziel	2
1.2 Methodischer Ansatz	2
1.3 Struktur dieser Arbeit	5
2 Theoretischer Hintergrund	7
2.1 Grundlagen Drohnentechnologie	7
2.1.1 Zuladung	9
2.1.2 Reichweite	9
2.1.3 Automatisierte Navigation	10
2.1.4 Kameratechnik	11
2.2 Grundlagen der Informationssicherheit	12
2.2.1 CIA-Triade	13
2.2.2 STRIDE-Modell	14
3 Verwandte Arbeiten	15
4 Literaturanalyse	19
4.1 Methode	20
4.2 Bedrohungen aus der Literatur	21
4.2.1 Mitlesen von sensiblen Informationen	21
4.2.2 Mithören von sensiblen Informationen	22
4.2.3 Abfangen von Funksignalen	23
4.2.4 Senden von Funksignalen	23
5 Experteninterviews	25
5.1 Methode	25
5.1.1 Struktur der Interviews	25
5.1.2 Aufbau des Fragenkatalogs	26

5.1.3	Analyse des Inhalts	27
5.2	Ergebnisse der Experteninterviews	29
5.2.1	Kameratechnik	29
5.2.2	Funktechnik.....	31
5.3	Klassifizierung.....	32
6	Praktischer Versuch.....	35
6.1	Ziel und Konzept.....	35
6.2	Durchführung	36
6.2.1	Rahmenbedingungen.....	37
6.2.2	Kernfrage Machbarkeit.....	39
6.2.3	Kernfrage Entdeckungsrisiko	42
6.2.4	Kernfrage Abwehr	44
7	Abwehrmaßnahmen	49
7.1	Übersicht.....	49
7.2	Herausforderungen	52
8	Diskussion	55
8.1	Vielfalt von Drohnenbedrohungen.....	55
8.2	Potenzial von Angriffen	56
8.3	Herausforderungen bei der Abwehr	57
8.4	Eintrittswahrscheinlichkeit von Drohnengefahren.....	58
8.5	Stand der Forschung des Fachgebietes.....	59
9	Fazit	61
	Literaturverzeichnis	63
	Abbildungsverzeichnis.....	71
	Tabellenverzeichnis.....	73
	Abkürzungsverzeichnis.....	75
	Versicherung über redliches wissenschaftliches Arbeiten.....	77
	Anhang.....	79
Anhang A	: Fragenkatalog	79

Anhang B : Datenschutzerklärung.....	81
Anhang C : Kodierleitfaden	83
Anhang D : Referenzblatt mit fiktiven sensiblen Informationen.....	85
Anhang E : Exemplarische Versuchsfragen	86
Anhang F : Screenshot der Fragenkatalog KI-Konversation.....	87
Anhang G : Monatsberichte	88

1 Einleitung

Wie in vielen Bereichen schreitet der technische Fortschritt auch im Segment der Drohnen stets voran. Drohnen werden immer erschwinglicher [1] und die Kameratechnik entwickelt sich stets fort [2]. Dieser Fortschritt bringt Vorteile für Unternehmen, die Drohnen zu vielseitigen Zwecken wie der Bewirtschaftung von Agrarflächen [3], der Inspektion technischer Anlagen, dem Verbringen von Waren zu logistischen Zwecken oder künftig auch im Bereich der Telekommunikation [4] einsetzen können. Auch für Privatpersonen bringt der Fortschritt in dieser Branche einen Vorteil. Drohnen können heutzutage zu vielen freizeitlichen Zwecken eingesetzt werden. So erfreuen sich unter anderem Hobbyfotografen den Vorzügen beim Erstellen qualitativ hochwertiger Aufnahmen [5]. Auch der Einsatz als Spielzeug oder das Fliegen von Drohnenrennen sind beliebte Einsatzgebiete für Privatpersonen [6]. Und auch in Zukunft wird uns der vermehrte Einsatz von Drohnen begleiten [7]. Doch nicht zuletzt der Ukraine-Konflikt zeigt [8]: Auch die maliziöse Seite der Gesellschaft profitiert vom technischen Fortschritt im Bereich der Drohnen [9]. Innerhalb von Deutschland lässt sich aktuell kein kriegerischer Einsatz von Drohnen beobachten. Trotzdem können die neuen Möglichkeiten von Drohnen auch in Deutschland eine Gefahr für Unternehmen darstellen. So berichtet der im Rahmen dieser Arbeit interviewte Experte für Werkschutz I1 folgendes.

„Ich würde, Stand jetzt, auch sagen, dass es aktuell in Deutschland sehr leicht ist, mit einer Drohne einen Angriff auf die IT-Sicherheit zu unterstützen.“ (I1, Pos. 9)

Ob und wie diese These in die Realität zu übertragen ist, soll im Rahmen dieser Arbeit untersucht werden. Hierzu wird Literatur analysiert, Experten interviewt und eine praktische Fallstudie durchgeführt, um das aktuelle Bedrohungspotenzial einzuschätzen. Außerdem werden Möglichkeiten zur Abwehr evaluiert, um somit ein aktuelles und künftiges Bild der Gefahrenlage von Drohnen auf die Informationssicherheit zu erlangen. Zum Schluss werden die Implikationen der Forschungsergebnisse auf den Fachbereich diskutiert und die Frage beantwortet, ob frei erhältliche Drohnen eine Gefahr für die Informationssicherheit in Organisationen darstellen. Die genaue Formulierung der Forschungsfrage und das Ziel dieser Arbeit sind Bestand des folgenden Kapitels.

1.1 Forschungsfrage und Ziel

Im Zentrum dieser Arbeit steht die Forschungsfrage, welches Gefahrenpotenzial frei erhältliche Drohnen für die Informationssicherheit von Organisationen darstellen. Hierzu sollen neben der Identifizierung möglicher Gefahren auch Abwehrmaßnahmen bewertet werden, um ein vollumfängliches Bild der Gefährdungslage zu bekommen.

Um die präzise Analyse des Fachbereichs zu ermöglichen, schränkt diese Arbeit die Untersuchungen in einigen Belangen ein und grenzt sich so von anderen Fachbereichen ab. Hierzu fokussiert sich diese Arbeit auf Drohnen, welche für Privatanwender mit vertretbarem Aufwand verfügbar sind. Dies schließt generell die Untersuchung von größeren Drohnen, welche beispielsweise zum Personentransport eingesetzt werden, aus. Wie sich im Verlauf dieser Arbeit zeigen wird, können Drohnen mit einer Vielzahl von Zuladungen bestückt werden. Auch hier beschränkt sich die Betrachtung auf frei erhältliche Zuladungen, der Grad der Spezialisierung wird hierbei jedoch nicht eingeschränkt.

Eine weitere Einschränkung im Rahmen dieser Arbeit ist die Motivation der Angreifer. Es wird davon ausgegangen, dass diese zwar maliziöse Zwecke verfolgen und sich nicht an gesetzliche Richtlinien halten, dabei jedoch moralischen Grundsätzen folgen. Dies schließt die Betrachtung von militärischen oder terroristisch motivierten Angriffen, wie dem Abwerfen von Sprengsätzen oder das absichtliche Steuern zur Induktion von Sach- oder Personenschäden aus. Des Weiteren konzentriert sich diese Arbeit in der Regel auf Organisationen, welche wirtschaftlich getrieben sind. Um für diese Art von Organisationen übertragbare Ergebnisse zu erreichen, ist auch der Einsatz militärischer Technologien bei der Abwehr nicht Teil dieser Arbeit.

Um die genannte Forschungsfrage vollumfänglich zu beleuchten, setzt diese Arbeit eine Reihe von methodischen Ansätzen ein. Diese werden im folgenden Kapitel erläutert.

1.2 Methodischer Ansatz

Diese Arbeit verfolgt methodisch einen vielschichtigen Ansatz, um eine vollumfängliche Betrachtung des Bedrohungspotenzials von Drohnen auf die Informationssicherheit zu ermöglichen. Das Fundament hierfür bildet eine Einführung in den theoretischen Hintergrund der Themengebiete Drohnen und Informationssicherheit, sowie das Evaluieren verwandter Arbeiten. Anschließend setzt diese Arbeit vier Schwerpunkte, um die Forschungsfrage zu beantworten.

Der erste Schwerpunkt liegt auf einer detaillierten Literaturanalyse. Hierbei wird relevante wissenschaftliche Literatur nach möglichen Angriffen durchsucht, welche mit Hilfe von Drohnen möglich wären. Es wird darauf geachtet, dass der unterstützende Einsatz von Drohnen bei der Durchführung eines Angriffs einen deutlichen Mehrwert bietet. Ziel hierbei soll es sein, exemplarisch einige hypothetische Angriffe zu identifizieren, um ein Gefühl für das Bedrohungspotenzial von Drohnen zu bekommen.

Den zweiten Schwerpunkt bildet die Durchführung von Experteninterviews. Diese Interviews sollen die Arbeit durch die Erfahrungen von Spezialisten in den Bereichen Informationssicherheit und Drohnen bereichern. Ziel ist es, durch den Austausch mit Experten aktuelle und praxisrelevante Erkenntnisse zu gewinnen, die über den Rahmen der verfügbaren Literatur hinausgehen. Die gewonnenen Erkenntnisse ergänzen viele Bereiche der Arbeit, wie die identifizierten Gefahren aus der Literaturanalyse oder Möglichkeiten bei der Abwehr im Rahmen späterer Kapitel.

Der dritte Schwerpunkt dieser Arbeit liegt auf der Durchführung einer praktischen Fallstudie. Diese soll weitere Aufschlüsse über das tatsächliche Bedrohungspotenzial eines ausgewählten Angriffsszenarios geben. Die Versuche richten sich hierbei an drei Kernfragen aus. Diese untersuchen die Machbarkeit und die Entdeckungswahrscheinlichkeit von Angriffen mit Drohnen. Außerdem wird im Rahmen der Kernfragen auch eine Abwehrmaßnahme evaluiert. Durch die Untersuchung dieser, soll eine Brücke zum letzten Schwerpunkt dieser Arbeit geschlagen werden.

Der vierte Schwerpunkt dieser Arbeit stellt einen Querschnitt der Möglichkeiten bei der Drohnenabwehr dar. Hierbei werden verschiedene technische und nicht technische Maßnahmen betrachtet, um einen prägnanten Überblick über die generelle Funktionsweise zu erhalten. Anschließend werden Herausforderungen im Bereich der Drohnenabwehr erläutert, um anhand der defensiven Seite der Drohnengefahren weitere Aussagen über deren Bedrohungspotenzial treffen zu können.

Um neue Gefahren identifizieren zu können und ein Lagebild der Gefahren zu erhalten, wählt diese Arbeit einen explorativen Ansatz. Dieser eignet sich im Gegensatz zu deskriptiven, explanativen oder evaluativen Ansätzen aufgrund der im folgenden Kapitel 3 festgestellten infantilen Lage der Forschung in diesem Bereich besonders gut [10].

Methodisch wird eine qualitative Forschungsstrategie herangezogen, da sich die Gefahren nur schwer quantitativ erfassen lassen. Um ein breiteres Bild der Gefahrenlage zu erhalten, wird zusätzlich ein multimethodischer Ansatz gewählt. Dieser verbindet die Erkenntnisse aus einer Reihe von Forschungsansätzen, um eine möglichst vielschichtige Betrachtung zu ermöglichen. Die gewählte Forschungsstrategie bei der Identifizierung von möglichen Gefahren ist hierbei dreispitzig. Mithilfe einer Literaturliteraturanalyse sollen bestehende Gefahren in der Literatur identifiziert werden. Zusätzlich sollen diese auf das untersuchte Themengebiet übertragen werden. Mithilfe einer Fallstudie soll eine der identifizierten theoretischen Gefahren in die Praxis umgesetzt und deren Machbarkeit belegt werden. Experteninterviews schlagen schließlich die Brücke zwischen theoretischem Fachwissen und Praxiserfahrungen und sollen den aktuellen Stand in Organisationen widerspiegeln. Abbildung 1 zeigt die von diesem Ansatz abgedeckten Gebiete, eingeordnet auf dem Spektrum von Theorie zu Praxis.

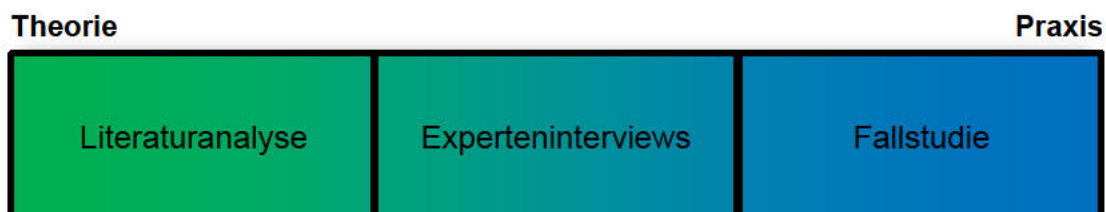


Abbildung 1: Übersicht der methodischen Ansätze

Der vierte Schwerpunkt dieser Arbeit beleuchtet thematisch die Gegenseite der drei vorherigen Ansätze. Er fokussiert sich hierbei vorwiegend auf die theoretischen Möglichkeiten. Bei der Betrachtung der Herausforderungen expandiert er jedoch auch in Richtung Praxis, wobei er jedoch nicht das Maß an Realitätsnähe der Fallstudie erreicht. Wie die verschiedenen Ansätze in die Gesamtstruktur dieser Arbeit einzuordnen sind, wird im folgenden Kapitel erläutert.

1.3 Struktur dieser Arbeit

Allgemein folgt die Struktur dieser Arbeit einem viersäuligen Bottom-Up Ansatz. Für ein vertieftes Verständnis der Struktur dieser Arbeit kann es vorteilhaft sein, sich diese Struktur visuell zu vergegenwärtigen. Den grundlegenden Aufbau dieser Arbeit stellt die folgende Abbildung 2 dar.

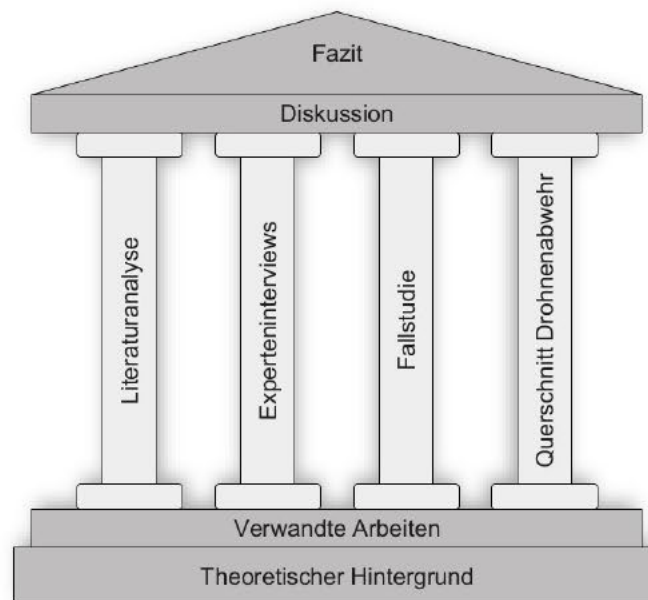


Abbildung 2: Darstellung der Struktur dieser Arbeit

Der Ausgangspunkt befindet sich im unteren Teil der Abbildung mit der Erläuterung des theoretischen Hintergrunds. Hier werden den Lesenden Grundlagen über die Funktionsweise von Drohnentechnologien vermittelt. Außerdem werden aktuelle technische Möglichkeiten mit Drohnen kurz erläutert. Zusätzlich werden Lesenden einige Kernkonzepte der Informationssicherheit nähergebracht. Dieses Fundament schafft für alle Lesenden einen gemeinsamen Ausgangspunkt zur Interpretation der Forschung im weiteren Verlauf dieser Arbeit.

Anschließend wird der aktuelle Stand der Forschung auf diesem Gebiet untersucht, um mögliche Forschungslücken zu identifizieren und die Sinnhaftigkeit dieser Arbeit herauszustellen. Hierzu werden drei thematisch verwandte wissenschaftliche Arbeiten betrachtet, deren Ergebnisse analysiert und die Relevanz im Kontext dieser Arbeit bewertet.

Auf Basis dieser Grundlage erweitert dann das darauffolgende Kapitel 4 den Fokus der betrachteten wissenschaftlichen Arbeiten. Dieses Kapitel stellt die erste Säule in Form der Literaturanalyse dar. Hierbei werden exemplarisch einige Angriffe aus der Literatur identifiziert, welche vom Einsatz von Drohnen bei der Durchführung profitieren. Um weitere mögliche Gefahren zu identifizieren, werden im nächsten Kapitel die

Meinungen von Experten erfasst. Dieses Kapitel umfasst die Konzeptionierung und Durchführung von sechs Fachinterviews mit Fachkundigen aus verschiedenen Arbeitsbereichen mit Schnittstellen zur Thematik „Drohne“.

Mithilfe einer qualitativen Inhaltsanalyse werden die weiteren Gefahren, welche von Experten identifiziert wurden, genannt und eingeordnet. Die Ergebnisse der Experteninterviews fließen außerdem, je nach Thematik, in weitere Teile dieser Arbeit ein. So profitiert der Teil der Abwehrmaßnahmen durch die Identifizierung spezieller, auf die Thematik zugeschnittener, Vorgehensweisen durch die Experten. Diese gingen aus der durchgeführten grundlegenden Literaturanalyse nicht hervor. Auch fließen sowohl kritische Expertenmeinungen als auch Aussagen über die künftige Entwicklung des Fachbereichs in den Teil der Diskussion ein.

Nach der Durchführung der Experteninterviews folgt die Planung und Durchführung der praktischen Fallstudie. Den Lesenden wird hierbei zu Beginn die Methodik und der Versuchsaufbau nähergebracht. Anschließend erfolgt die Darstellung der Ergebnisse anhand der Beantwortung von drei Kernfragen über die Machbarkeit, das Entdeckungsrisiko und die Effektivität einer Abwehrmaßnahme.

Die Diskussion über Abwehrmaßnahmen wird dann im folgenden Kapitel 7 ausgeweitet und fortgeführt. Hierzu werden verschiedene Möglichkeiten bei der Drohnenabwehr in Form technischer Systeme zur aktiven Abwehr, der Drohnerdetektion und in Form nichttechnischer Maßnahmen, welche von Experten identifiziert wurden, betrachtet.

Anschließend werden die Herausforderungen bei der Drohnenabwehr herausgestellt und die Komplexität bei der Entscheidungsfindung über Maßnahmen zur Drohnenabwehr dargestellt. Der Abschluss dieses Kapitels schließt auch den datenerhebenden Teil dieser Arbeit und eröffnet im darauffolgenden Kapitel die Diskussion der Ergebnisse. Hierbei stellt die Arbeit fünf Kernerkenntnisse als Ergebnis dieser Forschung heraus. Deren Implikationen werden bewertet, eingeordnet und kritisch betrachtet.

Die Arbeit schließt mit dem Fazit. Hier wird prägnant das Vorgehen sowie die maßgeblichen Forschungsergebnisse dargestellt. Außerdem wird hier die Notwendigkeit weiterer Forschung auf dem untersuchten Gebiet vorgestellt und die einzelnen möglichen Forschungsrichtungen benannt.

2 Theoretischer Hintergrund

Um mögliche Bedrohungen durch Drohnen auf die Informationssicherheit identifizieren und bewerten zu können, ist es sinnvoll, einige Grundlagen der beiden Fachbereiche zu verstehen und sich die technischen Möglichkeiten von Drohnen vor Augen zu führen. Mit diesem Verständnis ist es in den späteren Teilen möglich, Bedrohungen technisch fundiert zu identifizieren und in den Kontext der Informationssicherheit einzuordnen. Zudem wird es thematisch ferneren Lesenden ermöglicht, die Forschung im Verlauf dieser Arbeit einfacher nachzuvollziehen. Genau diesen theoretischen Hintergrund bietet das folgende Kapitel.

2.1 Grundlagen Drohnentechnologie

Um Drohnentechnologien grundsätzlich zu verstehen, wird das Wort „Drohne“ an sich zu Beginn definiert werden. Die Literatur bietet eine Reihe verschiedener Definitionen. Eine lautet wie folgt: *"Aerial vehicles that do not carry a human operator, fly remotely or autonomously, and carry lethal or nonlethal payloads are considered as drones"* [11, p. 1]. Hierbei ist es wichtig zu verstehen, dass Drohnen in Bauform, Größe und technischer Ausstattung sehr divers sind. So identifiziert [11] beispielsweise sechs Überkategorien von Drohnen. Diese teilen sich, je nach Bauart, in jeweils bis zu 21 verschiedene Unterkategorien. Die Vielfältigkeit der Bauweisen wird in der folgenden Abbildung 3 durch einige ungewöhnliche, nicht näher erläuterte Beispiele dargestellt.



Abbildung 3: Verschiedene Bauformen von Drohnen aus [12]

Nicht zuletzt aufgrund dieser Varietät in ihrer Bauform, sondern auch aufgrund ihrer flexiblen Einsatzmöglichkeiten und ihrer Geschwindigkeit finden Drohnen in vielen Bereichen Anwendung. Diese Anwendungsgebiete umfassen unter anderem Logistik, Agrarwirtschaft oder Bevölkerungsschutz. Um eine einfache Betrachtung dieser Vielfalt zu ermöglichen, teilt [12] diese Einsatzgebiete in die Kategorien „Militärisch“, „Kommerziell“ und „Industrie“ ein. Die folgende Abbildung 4 zeigt beispielhaft jeweils eine Drohne aus der von [12] identifizierten Kategorien. Der linke Teil der Abbildung zeigt den militärischen Einsatzzweck in Form der „EMT Luna X 2000“ Aufklärungsdrohne. Der Einsatz von Drohnen zu industriellen Zwecken ist auf dem rechten Teil der Abbildung in Form der „DJI Agras T30“ Agrardrohne dargestellt. Der untere Teil der Abbildung zeigt die „DJI Mavic 3 Pro“, eine Drohne zur kommerziellen Anwendung. Drohnen dieser Kategorie werden beispielsweise zum Erstellen von Bild- und Videoaufnahmen aus der Luft eingesetzt werden.



Abbildung 4: Beispiele der verschiedenen Drohnenkategorien aus [13–15]

Im Rahmen dieser Arbeit sollen ausschließlich Drohnen betrachtet werden, welche auch für private Akteure frei erhältlich sind. Diese fallen vorwiegend in die Kategorie „Kommerziell“. Aber auch einige Drohnen der Kategorie „Industrie“ sind frei erhältlich. Diese sind daher auch Teil der Betrachtung dieser Arbeit. Neben Drohnen als fertiges Produkt, umfasst die Erhältlichkeit auch einzelne Bauteile, die zum Bau einer Drohne verwendet werden können.

Nebst der Verfügbarkeit und Bauform ist die technische Ausstattung eines Drohnensystems von besonderer Relevanz. In ihr liegt hauptsächlich das mögliche Gefahrenpotenzial. Einige mögliche Zuladungen werden im folgenden Unterkapitel beschrieben.

2.1.1 Zuladung

Die Zuladung (auch „Payload“) einer Drohne beschreibt alle zusätzlichen Ausstattungen einer Drohne, die nicht für den Flug benötigt werden. Hierzu zählen unter anderem zusätzliche Sensorik, Abwurfmechanismen, zusätzliche Kameras etc. Die Zuladung einer Drohne ist hinsichtlich Vielfalt allein beschränkt durch die Tragfähigkeit der Drohne. Diese Tragfähigkeit variiert je nach Bauform und technischer Ausstattung. So können laut [12] größere, zweiflüglige Drohnen, Zuladungen von bis zu einer Tonne verbringen. Die Zuladung von Drohnen mit Bauformen, welche in der Regel in frei erhältlichen Drohnen zu sehen sind, geben die Verfassenden mit 3,5 kg an. Einige Beispiele für Zuladungen sind (multispektrale) Kameras, Scheinwerfer, Lautsprecher, Sprühhvorrichtungen für Düngemittel oder Löschwasser, Sensoren wie LiDAR, Gas Sensorik oder weitere Zuladungen. Neben den vielfältigen Einsatzmöglichkeiten bieten Drohnen auch eine hohe Reichweite, in der diese Zuladungen eingesetzt werden können. Die Reichweite wird in dem folgenden Unterkapitel beschrieben.

2.1.2 Reichweite

Die Reichweite beschreibt die maximale Distanz, welche ein Pilot zu seiner Drohne haben kann, um diese zu kontrollieren. Viele frei erhältliche Drohnen sind meist über zwei Funkstrecken mit dem Piloten verbunden. Eine überträgt dabei Steuerbefehle, um die Bewegungen der Drohne zu kontrollieren. Die andere überträgt einen Videostream, um dem Piloten ein Bild des Umfeldes der Drohne zu geben. Beide Funkstrecken haben Limitationen bezüglich ihrer Distanz. Da die Funkübertragung des Videofeeds deutlich mehr Daten übertragen muss, ist diese oft der limitierende Faktor bei der Übertragungreichweite. Gängige Systeme zur Videoübertragung wie das sog. „DJI O3 Pro System“ [16] haben laut Hersteller eine Reichweite von bis zu 15 Kilometern.

Benötigen Piloten keine Echtzeit-Videoübertragung, so ist die Reichweite deutlich erweitert, mit bis zu 35 Kilometern [17] in frei erhältlichen Systemen wie ELRS. Auch der Einsatz von Mobilfunk oder Satellitenkommunikation zur Übermittlung von Steuerbefehlen ist möglich. Die Reichweite ist je nach Netzabdeckung hierbei praktisch unbegrenzt. Die Übermittlung von Echtzeit-Videosignalen mittels LTE gestaltet sich aktuell aufgrund der hohen Latenz als herausfordernd. Mit dem weiteren

Voranschreiten des 5G-Ausbaus könnte diese Art der Steuerung jedoch in Zukunft vermehrt Anwendung finden [18].

In Szenarien, in denen Drohnen eine höhere Distanz zurücklegen müssen, ist die Navigation ohne visuelle Anhaltspunkte herausfordernd. Hier muss sich anderer Methoden zur Steuerung bedient werden. Dazu ermöglicht frei erhältliche Technik eine teilautonome Navigation mittels GPS. Da die Steuerbefehle dabei nicht in Echtzeit übertragen werden müssen, können Kommunikationstechnologien mit einer größeren Reichweite eingesetzt werden. Die technischen Möglichkeiten der teilautonomen Navigation werden im folgenden Unterkapitel erläutert.

2.1.3 Automatisierte Navigation

Automatische Drohnen, nicht zu verwechseln mit autonomen Drohnen, sind in der Lage, vom Piloten im Voraus festgelegte Aufgaben eigenständig zu erfüllen [19]. Im Gegensatz zu autonomen Drohnen muss der Pilot im Falle eines unvorhergesehenen Ereignisses jedoch eingreifen. Es gibt bereits einige quelloffene Software [20], welche die automatische Navigation von Drohnen mittels GPS ermöglicht. Die nachfolgende Abbildung 5 illustriert beispielhaft einige Möglichkeiten dieser Art von Software. So können in dieser Ground Control Station Software Projekts „Ardupilot“ Missionen mit

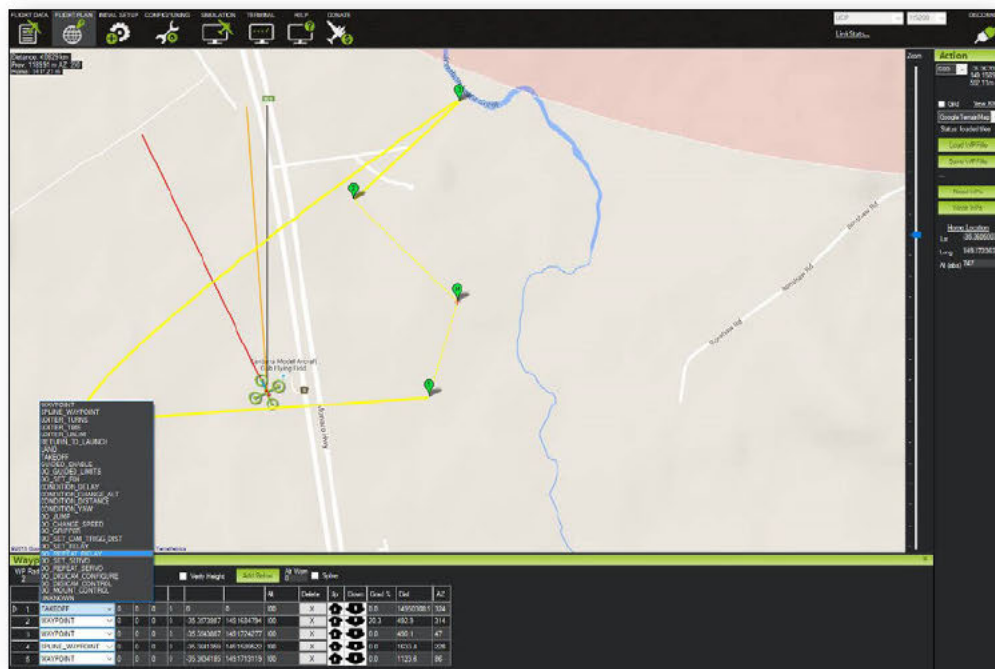


Abbildung 5: Ardupilot Mission Planner aus [21]

vorgefertigten Flugrouten erstellt werden. Mittels Wegpunkten können dann auf Punkten der Route Aufgaben ausgeführt werden, wie das Abwerfen von Nutzlasten oder das Auslösen einer Bordkamera. Wie genau die technischen Beschaffenheiten von Bordkameras in Drohnen sein können, wird im folgenden Kapitel erläutert.

2.1.4 Kameratechnik

Das Herzstück vieler Drohnen für den Privatgebrauch ist die Bordkamera. Grundsätzlich können Drohnen mit der richtigen Ausstattung beliebige Kameratechnik transportieren. So sind 3D druckbare Baupläne für Stabilisierungsvorrichtungen für hochauflösende DSLR-Kameras bereits öffentlich zugänglich. Die Verfügbarkeit von montagefertigen Vorrichtungen für größere Kameras ist jedoch auf dem freien Markt vergleichsweise gering. Flugfertige Drohnen mit eingebauter Kamera sind jedoch allgemein sehr einfach verfügbar. Um exemplarisch einen Überblick über Drohnen mit eingebauter Kameratechnik zu erhalten, wird in Tabelle 1 ein kurzer Ausschnitt einiger aktueller Drohnensysteme gegeben. Zusätzlich wird eine Preisindikation für jedes Modell angegeben. Die Preise orientieren sich hierbei an verfügbaren Online-Angeboten zum Zeitpunkt der Verfassung dieser Arbeit. Die Tabelle gibt außerdem das Zoomlevel jeder Drohne an. Bei diesem gilt es den digitalen und optischen Zoom zu unterscheiden. Optischer Zoom findet bereits innerhalb des Objektivs der Kamera statt und führt zu einer verlustfreien Vergrößerung des Motivs. Der digitale Zoom vergrößert durch Nachbearbeitung des Bildes nachträglich. Dabei sind bei der vergrößerten Ansicht keine neuen Informationen verfügbar. Das digitale Zoomen eines Bildes ähnelt dem Nutzen eines großen Bildschirms oder dem Heranzoomen eines Bildes auf einem Smartphone. In der Regel setzen die Drohnenkameras zuerst den optischen Zoom ein. Nachdem die maximale optische Zoomstufe erreicht wurde, wird das Bild mit Hilfe des digitalen Zooms künstlich weiter vergrößert. Eine Übersicht über die verschiedenen Zoomstufen verschiedener Drohnenkameras wird in der folgenden Tabelle 1 dargestellt.

Firma	Modell	Preispunkt	Optischer Zoom	Digitaler Zoom
DJI	Mini 3 Pro	745 €	1x	4x
Autel Robotics	EVO Lite+	876 €	1 - 3x	3x - 16x
DJI	Mavic 3 Pro	2.099 €	1 - 7x	7x - 28x
YUNEEC	H520E + E30ZX	5.800 €	1 - 30x	30x - 36x
Parrot	Anafi USA	8.330 €	1 - 5x	5x - 32x

Tabelle 1: Preisvergleich verschiedener Kameratechniken

Die Leistungsfähigkeit eines der oben aufgeführten Kamerasysteme ist in der folgenden Abbildung 6 dargestellt. Das im letzten Bild abgebildete Haus befindet sich in ca. 2 km Entfernung zur Drohne. Die Schriftzeichen auf der Vergrößerung sind schemenhaft erkennbar.



Abbildung 6: 36x Zoom der E30ZX (ca. 2 km Distanz) aus [22]

Diese optischen Möglichkeiten, gemeinsam mit der Vielzahl verschiedener Zuladungen, der hohen Reichweite, sowie der Möglichkeit zur automatisierten Navigation, stellen Drohnen als vielseitige Plattform dar. Anhand der Abbildung 7 lässt sich auch vermuten, dass der Einsatz von Drohnen zur Beeinträchtigung der Informationssicherheit ebenfalls möglich ist. Was den Begriff der Informationssicherheit umfasst, wird im folgenden Kapitel näher erläutert.

2.2 Grundlagen der Informationssicherheit

Um Informationssicherheit zu verstehen, ist es sinnvoll, sich der Betrachtung einer Definition zu bedienen. In der Literatur ist folgende Definition zu finden: „Die **Informationssicherheit** zielt auf den angemessenen Schutz von Informationen und IT-Systemen insbesondere in Bezug auf alle festgelegten Schutzziele, wie Vertraulichkeit, Integrität und Verfügbarkeit, ab. So soll insbesondere ein unbefugter Zugriff oder Manipulation von Daten verhindert und soweit möglich vorgebeugt werden, um daraus

resultierende wirtschaftliche Schäden zu verhindern. Bei den Daten ist es unerheblich, ob diese einen Personenbezug haben oder nicht. Informationen können sowohl auf Papier oder in IT-Systemen vorliegen.“ [23, p. 2]

Neben dem Begriff der Informationssicherheit definiert die Autorin außerdem die Begriffe IT-Sicherheit und Datenschutz separat. Diese beiden Begriffe werden gelegentlich als Synonym für den Begriff der Informationssicherheit verwendet, sind jedoch nur Teilmengen dieser. Im Gegensatz zur IT-Sicherheit umfasst Informationssicherheit alle Arten von Informationen in jeglicher, auch Nichtdigitaler, Form. Die Definition nennt zudem die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Diese Schutzziele bieten eine wichtige Grundlage in der Informationssicherheit [24] und sind eines der Kernkonzepte des Fachgebiets. Sie werden im Rahmen der sogenannten CIA-Triade im nächsten Unterkapitel genauer erläutert.

2.2.1 CIA-Triade

Die CIA-Triade ist wie die Pfeiler der Informationssicherheit zu betrachten. Das Akronym steht hierbei für die Schutzziele „**C**onfidentiality“ (Vertraulichkeit), „**I**ntegrity“ (Integrität) und „**A**vailability“ (Verfügbarkeit) [25].

Der Begriff „Vertraulichkeit“ beschreibt dabei, dass Informationen gegen den Zugriff von Unberechtigten geschützt sein müssen. Ist die Vertraulichkeit von Informationen einmal verloren, kann sie nicht wiederhergestellt werden. Eine Verletzung der Vertraulichkeit ist etwa der Versand von vertraulichen Dokumenten an den falschen Empfänger.

Die „Integrität“ beschreibt die Unverfälschbarkeit von Daten. Ist dieses Schutzziel erfüllt, so können Informationen nicht versehentlich oder von Unberechtigten geändert werden. Ändert etwa ein Kunde einer Bank unbefugt seinen eigenen Kontostand, so ist dies ein Bruch der Integrität.

Die „Verfügbarkeit“ beschreibt deskriptiv, dass Informationen dann zugreifbar sind, wenn sie benötigt werden. Ein ungeplanter Ausfall der Lernplattform einer Hochschule, bspw. aufgrund von Hochwasser, stellt eine Verletzung der Verfügbarkeit dar, da Nutzer zur Zeit des Ausfalls nicht auf die Informationen des Systems zugreifen können.

Das CIA-Modell wird vor allem im defensiven Kontext zum Schutz von Informationen eingesetzt. Ein weiteres Kernkonzept der Informationssicherheit ist das STRIDE-Modell. Dieses kategorisiert Gefahren, welche die Informationssicherheit beeinträchtigen können. Die beiden Modelle sind nicht als gegensätzlich zu betrachten, sondern

haben einige Schnittmengen und komplementieren sich. Das STRIDE-Modell wird im folgenden Unterkapitel erläutert.

2.2.2 STRIDE-Modell

Wie CIA ist auch STRIDE ein Akronym. Im Fall von STRIDE beschreiben diese keine Schutzziele, sondern dienen der Kategorisierung von Bedrohungen, welche die Informationssicherheit beeinträchtigen können. Das Modell unterscheidet folgende Kategorien:

- **Spoofing:** z. B. Angreifer kann E-Mails im Namen anderer versenden
- **Tampering:** z. B. unberechtigtes Ändern von Daten
- **Repudiation:** z. B. in einem Chatportal ist nicht nachvollziehbar, wer eine Nachricht gesendet hat
- **Information Disclosure:** z. B. unberechtigtes Lesen von Daten
- **Denial of Service:** z. B. DDoS Angriff
- **Elevation of Privileges:** z. B. Angreifer kann sich selbst Administratorberechtigungen zuweisen

Durch den Einsatz von CIA in Kombination mit dem STRIDE-Modell können die Gefahren genauer zugeordnet werden, da sowohl die defensive als auch die offensive Seite der Gefahr eingestuft wird.

Im weiteren Verlauf dieser Arbeit werden mögliche Gefahren durch Drohnen identifiziert. Um diese in den Kontext der Informationssicherheit bringen zu können, wird jeder Angriff in die beiden Modelle eingeordnet.

Mithilfe dieser Grundlagen kann die Forschung im weiteren Verlauf dieser Arbeit besser nachvollzogen werden. Außerdem hilft dieses Verständnis dabei, das Ziel und die Forschungsfrage dieser Arbeit in den aktuellen Forschungsstand auf diesem Gebiet einzuordnen. Diese Einordnung erfolgt im folgenden Kapitel.

3 Verwandte Arbeiten

Um die Nützlichkeit und Relevanz dieser Arbeit einzuschätzen, wird das Forschungsziel in diesem Kapitel in den aktuellen Stand der Forschung eingeordnet. Hierzu wurden einige thematisch verwandte Arbeiten identifiziert und analysiert. Die Ergebnisse dieser Arbeiten werden im Folgenden kurz zusammengefasst. Außerdem wird deren Relevanz für diese, vorliegende Arbeit, beschrieben und die Themengebiete voneinander abgegrenzt. Während der Recherche verwandter Arbeiten konnte festgestellt werden, dass die allgemeine Forschungslage im untersuchten Bereich aktuell noch dünn ist. Es konnten daher lediglich drei Arbeiten identifiziert werden, welche eine hinreichende Ähnlichkeit zum Forschungsziel dieser Arbeit aufweisen.

Sethuraman, Vijayakumar und Walczak untersuchen in Ihrem 2020 veröffentlichten Paper „*Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles*“ [26], wie Drohnen eingesetzt werden können, um tragbare medizinische Geräte anzugreifen. Im Praxisversuch des Papers gelang es dem Team einen „Drone-in-the-Middle-Angriff“ mittels Rogue Accesspoint auszuführen und Daten von medizinischen Geräten wie Pulsmesser mitzuschneiden. Sie demonstrierten zudem zwei Denial of Service Angriffe auf Ressourcen in einer simulierten Smart-Hospital-Umgebung.

Auch wenn die Verfassenden im Praxisversuch einen Angriff mittels WLAN durchführen, erwähnen Sie explizit das Gefahrenpotenzial für mittels Body Area Network (z. B. Bluetooth) vernetzte sowie implantierte Geräte. Sie unterstreichen hierdurch den Mehrwert, den Drohnen bei Angriffen liefern können, indem sie Hardware an sonst schwer zu erreichbare Orte bringen. Die Arbeit beschränkt sich thematisch rein auf den Kontext der Sicherheit im Medizinbereich. Auch die Schutzziele sowie weitere mögliche Angriffe werden nicht betrachtet.

In ihrer 2022 veröffentlichten Arbeit „*Unmanned Aerial Vehicles as a Source of Information Security Threats of Wireless Network*“ [27] untersuchen Serhii Voitenko, Volodymyr Druzhylin, Hanna Martyniuk und Tetiana Meleshko die Gefahren von Drohnen für Mobilfunknetzwerke. Die Forschenden identifizieren dabei drei Typen von Drohnen, die sich jeweils in Ihrer Zuladung unterscheiden. Diese sind Aufklärungsdrohnen, Drohnen für die elektronische Kriegsführung und sog. „Schock“ Drohnen. Aufklärungsdrohnen sind hierbei mit Kameras ausgestattet und sollen der Vertraulichkeit abtragen. Drohnen für die elektronische Kriegsführung tragen schwere Funktechnik und sollen Jamming sowie Spoofing Angriffe durchführen können. „Schock“ Drohnen sollen durch physische Beschädigung oder Beeinträchtigung das Schutzziel der Verfügbarkeit verletzen. Am Ende der Arbeit weisen die Verfassenden den

Angriffen ein Schadenspotenzial sowie eine Eintrittswahrscheinlichkeit zu. Das größte Risiko geht laut den Verfassenden von einem Spoofing-Angriff der elektronischen Kriegsführungsdrohne aus. Die Verfassenden stellen ein ernst zu nehmendes Risiko für 4G-Netzinfrastruktur fest.

Die Arbeit zeigt, wie verschiedenen Zuladungen von Drohnen dazu verwendet werden könnten, um die Schutzziele der IT-Sicherheit anzugreifen. Im Verlauf der Arbeit nennen die Forschenden hierbei keine Zwischenfälle aus der Praxis und halten die Angriffe zwar realitätsgetreu, aber eher hypothetisch. Die betrachteten Drohnen und Funkhardware in dieser Arbeit weisen außerdem einen hohen Grad an Spezialisierung auf. Da die Angriffe auch destruktiver Natur sind, kann davon ausgegangen werden, dass die Verfassenden auch von militärischen Angreifern ausgehen. Die Arbeit behandelt ebenso nur Angriffe im Bereich der Mobilfunktechnik. In Sachen Professionalität der Angreifer und untersuchtem Themengebiet sind deutliche Unterschiede zu dieser Arbeit festzustellen.

In ihrem wissenschaftlichen Artikel [28] untersuchen Swinney und Woods 2022, Arten von Drohnenzwischenfällen und Abwehrmöglichkeiten. Sie stellen hierbei zweifelsfrei fest, dass die künftige Relevanz durch das exponentielle Wachstum im kommerziellen Drohnenmarkt bis 2028, gegeben ist. Des Weiteren unterstreichen sie die Relevanz durch die Aufzählung zahlreicher Zwischenfälle mit Drohnen. Bei der Untersuchung der Zwischenfälle gruppieren die Forscher die Zwischenfälle in die Kategorien „physischer Angriff“, „Cyberangriff“, „Störung“ und „Ausspähen“. Im weiteren Verlauf der Arbeit werden außerdem diverse Möglichkeiten zur Detektion von Drohnen mithilfe von Technologien wie Radar, LiDAR und Funk sowie Audio- und Videosignalen untersucht. Die Arbeit geht hierbei detailliert auf die einzelnen Erkennungsansätze ein. Abschließend werden einige Möglichkeiten zur Drohnenabwehr untersucht und kritisch bewertet. Die Arbeit kommt zu dem Schluss, dass die Anzahl an Zwischenfällen in den vergangenen Jahren gestiegen ist. Sie stellt zudem fest, dass es aktuell keinen einzelnen Ansatz zur Detektion gibt, welcher zuverlässig funktioniert. Die Forscher schlagen daher weitere Forschung vor, um die einzelnen Detektionsansätze zu verbinden. Zudem stellen sie deutlich Hürden bei der Abwehr von Drohnen fest.

Der Artikel bestätigt die Relevanz dieser Arbeit, indem er die steigende Anzahl an Zwischenfällen allgemein hervorhebt. Ein Großteil der hierbei untersuchten Vorkommnisse fällt jedoch in die Kategorie der physischen Angriffe oder der Störung. Auch wenn die Begrifflichkeit „Störung“ mit dem Schutzziel der Verfügbarkeit in Verbindung gebracht werden kann, ist im Artikel oft von Störungen im physischen Betrieb

des Geschäftes und nicht der IT gemeint. Zwei der vier Kategorien liegen daher außerhalb des Rahmens dieser Arbeit. Während der Fokus des Artikels auf der Lageerfassung von Detektion und Abwehr liegt, untersucht diese Arbeit das mögliche Gefahrenpotenzial von Drohnen auf die Informationssicherheit. Der Forschungsschwerpunkt dieser Arbeit und des Artikels unterscheidet sich also deutlich.

Durch die Analyse weiterer verwandter Arbeiten konnte der Stand der Forschung im Bereich der Informationssicherheit in Bezug auf Drohnen erfasst werden. Hierbei wurde auch festgestellt, dass in diesem Kontext hauptsächlich drei Bereiche umfassend erforscht sind. Zum einen ist dies der Bereich der Härtung von Drohnen gegen Cyberangriffe. Die Arbeit in diesem Bereich ist vielfältig. So wird unter anderem die Hardwaresicherheit von Drohnen zur Absicherung gegen Angriffe untersucht ([29, 30]). Aber auch die Sicherheit von Drohne-zu-Drohne sowie Drohne-zu-Steuerung Kommunikation fallen in diese Kategorie ([29, 31–33]). Des Weiteren wurde der destruktive, militärische Einsatz von Drohnen bereits in einigen Arbeiten untersucht ([34, 35]). Die Forschung zu Möglichkeiten des Terrorismus ist hierbei ähnlich erforscht wie die der Terrorismusabwehr. Beide Bereiche sind aufgrund ihres destruktiven Charakters nicht Teil dieser Arbeit.

Die Forschung im Bereich der Drohnenerkennung ist ebenfalls vorangeschritten. Eine Reihe von Arbeiten schlagen diverse Ansätze zur Erkennung von Drohnen vor. Der Einsatz von Technologien wie KI oder Methoden zur Erkennung ist hierbei vielfältig. Im Kapitel 7 wird auf einige dieser Ansätze kurz eingegangen [36–38].

Die Gefahren von Drohnen für die Informationssicherheit sind bisher in der Forschung weitestgehend wenig untersucht. So untersuchen Arbeiten dieser Art jeweils sehr spezifische, einzelne Angriffe und bieten keinen Gesamtüberblick über die aktuelle Lage [26]. Andere Arbeiten untersuchen den Einsatz zerstörerischer Maßnahmen gegen drahtlose Informationstechnik [27].

Die genannten Felder der Forschung unterscheiden sich maßgeblich von der in dieser Arbeit untersuchten Materie. So soll sich diese Arbeit rein auf Gefahren für die Informationssicherheit beschränken. Die Beeinträchtigung dieser durch destruktive Maßnahmen oder Personengefährdung soll nicht untersucht werden. Die Abstinenz von Forschungsarbeiten in diesem Bereich stellt daher eine deutliche Forschungslücke im Bereich der Gefahren von Drohnen auf die Informationssicherheit dar. Um diese Lücke zu schließen, sollen im folgenden Teil dieser Arbeit Angriffs- und Verteidigungsmöglichkeiten analysiert werden. Den ersten Ansatz zur Identifikation möglicher Gefahren bildet die Literaturanalyse im nun folgenden Kapitel.

4 Literaturanalyse

Wie auch im Teil 2.1 Grundlagen Drohnentechnologie gezeigt, gilt es bei der Identifizierung von Gefahren von Drohnen auf die Informationssicherheit, zu beachten, dass Drohnen mobile Plattformen sind. Ähnlich wie bei anderen mobilen Plattformen, wie etwa dem PKW, bietet diese Mobilität eine Vielzahl verschiedener Einsatzmöglichkeiten. Definiert man einen PKW als ein motorisiertes Fahrzeug mit vier Rädern, so zählt sowohl ein Krankenwagen als auch ein militarisierter Pick-up einer Terrororganisation als PKW. Die Zuladung in Form von medizinischem Equipment zur Notfallversorgung kann Menschenleben retten und ist ein gesellschaftlich positiver Einsatzzweck. Bei einem Pick-up mit einer Zuladung in Form von 32 S5 Raketen, kann bei maliziöser Intention, von einem gesellschaftlich negativen Einsatz ausgegangen werden. Das Gefahrenpotenzial ist also weniger abhängig vom Vehikel selbst, sondern eher von der Zuladung sowie der Intention des Steuernden. Diese Zuladung kann je nach Kreativität des Angreifers beliebige Formen annehmen.

Bei der Betrachtung des Gefahrenpotenzials von Drohnen ist außerdem zu bedenken, dass Drohnen die Eigenschaft haben, viele physische Sicherheitsmechanismen durch ihre Flugfähigkeit zu umgehen. Dies ist insofern einzigartig, als dass es keine anderen Vehikel gibt, die dieses Ziel so kosteneffizient, intuitiv und risikoarm erreichen.

Unter Beachtung dieser Gegebenheiten werden im Folgenden nun exemplarisch einige Gefahren mit Hilfe von Literatur identifiziert. Um alle im Rahmen dieser Arbeit identifizierten Gefahren kompakt darzustellen, werden diese abschließend zusammen mit den Metriken geschätzte Kosten, geschätztes Schadenspotenzial, sowie technischer Komplexität dargestellt. Zudem werden die bei erfolgreicher Durchführung beeinträchtigten Schutzziele aus dem STRIDE sowie dem CIA-Modell aufgeführt. Diese Gefahren-Tabelle (Tabelle 3) konsolidiert zum einen die Ergebnisse aus diesem Kapitel sowie aus dem darauffolgenden Kapitel 5 Experteninterviews. Sie befindet sich daher an dessen Ende.

Wie genau die Gefahren in diesem Kapitel identifiziert werden, wird im folgenden Absatz über die Methode erläutert.

4.1 Methode

Der Teil der Literaturanalyse unterscheidet sich vom Kapitel 3 Verwandte Arbeiten insofern, als die Thematik der untersuchten Arbeiten nicht direkt mit dem Forschungsziel dieser Arbeit übereinstimmen muss. So sollen mögliche Angriffe identifiziert werden, welche vom Einsatz von Drohnen profitieren könnten. Ziel hierbei ist es nicht, eine vollumfängliche, systematische Literaturanalyse durchzuführen. Stattdessen sollen einige Gefahren exemplarisch identifiziert werden, um einen Eindruck der Gefährdungslage zu erhalten.

Die Auswahl der analysierten Literatur erfolgte hierbei nach folgendem Google Scholar Suchstring: „allintitle: attack cyber OR Information OR security OR drone -detection -defense -test -framework -politics -attribution“. Der verwendete Suchstring schließt gezielt bereits innerhalb der untersuchten Arbeit hypothetische Szenarien sowie Möglichkeiten zur Verteidigung aus. Auch Möglichkeiten zur Drohnenerkennung, abstrakte Frameworks, sowie politische Implikationen vom Einsatz von Drohnen sollen ausgeschlossen werden. Dies soll die Praxisrelevanz sicherstellen und die Machbarkeit durch den Ausschluss ungetesteter Angriffe erhöhen. Die Suchergebnisse wurden zusätzlich nach Veröffentlichungsdatum gefiltert. Dieses beschränkt sich hierbei auf den Zeitraum 2020 – 2023. In einem zweiten Schritt wurden dann die in diesen Arbeiten referenzierten Quellen gesichtet und weitere relevante Arbeiten untersucht. Um den Rahmen dieser Arbeit einzuhalten, folgte die Literaturrecherche einer ausschließenden Methodik. Kriterien zum Ausschluss sind:

- Angriffe, welche bereits innerhalb der untersuchten Literatur als hypothetisch gelten
- Angriffe auf Ziele außerhalb der Informationssicherheit
- Destruktive Angriffe oder solche, die eine direkte Gefährdung für Leib und Leben darstellen
- Angriffen, die zur Durchführung Hardware mit einem Gewicht über 1000 g benötigen
- Angriffe, bei denen Drohnen keinen signifikanten Mehrwert bieten

Anhand dieser Kriterien lassen sich zum Zeitpunkt der Erstellung ca. 1.750 wissenschaftliche Arbeiten identifizieren. Davon wurden im Rahmen dieser Arbeit ca. 100 Arbeiten grundlegend gesichtet. Durch die Anwendung der Ausschlusskriterien flossen schlussendlich ca. 10 % dieser Arbeiten in den nun folgenden Abschnitt ein.

4.2 Bedrohungen aus der Literatur

Während der Literaturanalyse wurden vier maßgebliche Kategorien identifiziert. Diese lassen sich grundlegend in die drei Überkategorien visuell, akustisch und Funk einteilen. Beginnend mit den visuellen Kategorien, werden diese in den folgenden Abschnitten auf Basis der Forschungsergebnisse der jeweils untersuchten Arbeiten erläutert. Außerdem werden mögliche Angriffe, welche sich aus den Forschungsergebnissen ableiten lassen, aufgezählt.

4.2.1 Mitlesen von sensiblen Informationen

In der 2018 veröffentlichten Arbeit „*Peeping Eye in the Sky*“ [39] untersuchten die Verfassenden die Möglichkeit, eingegebene PIN-Passwörter mithilfe von Videoaufnahmen und einem dafür entwickelten Algorithmus zu rekonstruieren. Dafür wurden Nutzer mittels Drohne durch ein Fenster gefilmt. Die Forschenden erreichten dabei auf eine Distanz von 15 Metern eine Erfolgsquote von 100 % innerhalb der ersten drei Passwortversuche. In einem weiteren Whitepaper [40] konnten die Forschenden eingegebene Passwörter mithilfe eines statischen Camcorders auf eine Distanz von 43 Metern bei 30 Durchläufen mit einer Präzision von 100 % bestimmen. Da seit der Veröffentlichung dieser Arbeiten jeweils fünf und elf Jahre vergangen sind, liegt die Vermutung nahe, dass diese Angriffe zum heutigen Zeitpunkt aufgrund des technischen Fortschritts noch effizienter wären. Das Mitlesen von Passworteingaben kann auf Basis dieser Forschungserkenntnisse als Bedrohung aufgenommen werden. Mithilfe des ausgespähten Passworts können Angreifer so Zugang zu technischen Systemen erlangen. Je nach System können Angreifer dann die Vertraulichkeit, die Integrität oder die Verfügbarkeit von Informationen einschränken. Bedenkt man den in 2.1.4 gezeigten aktuellen Stand derameratechnik, so ist das Mitlesen von Passwörtern ein ernstzunehmendes Risiko. Die Möglichkeit des Mitlesens muss sich hierbei nicht auf Passwörter begrenzen. Mit entsprechenderameratechnik können auch offen ausliegende Dokumente oder Bildschirminhalte fotografiert werden.

Weitere Arbeiten [41–43] untersuchten einen ähnlichen Angriff unter Verwendung speziellerameratechnik. Hierbei wurde die Effizienz von Angriffen mittels Wärmebildaufnahmen von Tastaturen, Trackpads und Touchscreens untersucht. Die Forschenden konnten dabei in bis zu 92 % der Fälle das eingegebene Passwort rekonstruieren [42]. Diese Art von Angriff setzt voraus, dass sich der Angreifer sehr nahe an dem Eingabegerät des Opfers befindet. Außerdem erhöht sich die Erfolgsquote der Angriffe, je näher der Aufnahmezeitpunkt des Bildes an der Eingabe des Passworts liegt. Auch diese Gefahr ist hypothetisch unter Einsatz von Drohnen möglich. Eine Drohne müsste sich hierzu jedoch entweder im Inneren eines Gebäudes

befinden oder die Eingabe durch ein geöffnetes Fenster beobachten, da die Wärmesignatur durch Fensterscheiben verfälscht wird. Der erfolgreiche unauffällige Angriff ist aufgrund des Fluggeräusches einer Drohne eher unwahrscheinlich. Jedoch könnten Angreifer die Drohne in der Nähe einer Eingabemöglichkeit unauffällig abstellen und die Geräusentwicklung durch das Ausschalten der Motoren eliminieren. Der Vollständigkeit halber wird dieser Angriff ebenfalls in die abschließende Gefahrentabelle mit aufgenommen.

4.2.2 Mithören von sensiblen Informationen

Neben Kameraequipment ist es Drohnen auch möglich Audioequipment als Zuladung zu transportieren. Dieser Ansatz mag aufgrund des signifikanten Fluggeräusches auf den ersten Blick unpraktikabel klingen. Die Fähigkeit von Drohnen, ihre Zuladung an schwer erreichbare Orte zu bringen, lässt das Angriffsszenario „Abhören“ jedoch realistisch erscheinen. Die Methodik, wie Audiosignale erfasst werden können, kann hierbei ebenfalls wieder sehr vielfältig sein. So könnten Angreifer Aufnahmegeräte wie Diktiergeräte oder Smartphones nahe an Fenstern platzieren. Die Rotorgeräusche, welche dabei die Aufnahmen verfälschen, können dann durch Abschalten der Motoren oder durch Abkoppeln und Wegfliegen der Drohne beseitigt werden. Anschließend können Informationen aus Gesprächen aufgezeichnet und abgehört werden. Auch der Einsatz eines gerichteten Mikrofons als Zuladung einer geschickt platzierten Drohne mit abgeschalteten Motoren ist in diesem Kontext denkbar. Ebenfalls ist der Einsatz von komplexeren Techniken wie die des Lasermikrofons mithilfe eines Laser-Doppler-Vibrometers möglich [44–46]. Dieses könnte als Nutzlast an einer exponierten Stelle gelandet und so ausgerichtet werden, dass das reflektierte Signal an einer zweiten Stelle aufgefangen werden kann.

Neben dem physikalischen Abhören von Schallwellen, kann auch Kameratechnik eingesetzt werden, um gesprochene Informationen zu erlangen. So könnten mithilfe einer hochauflösenden Kamera Aufnahmen vom Mund eines oder mehrerer Gesprächsteilnehmer gemacht werden. Diese können dann im Nachgang entweder mithilfe von Software [47] oder eines Experten analysiert, und so der Gesprächsinhalt extrahiert werden. In beiden Szenarien können so im Optimalfall bei erfolgreicher Durchführung vielfältige sensible Informationen über den Geschäftsbetrieb, mögliche Schwachstellen oder Details zu Systemen erlangt werden. Dies stellt eine Beeinträchtigung der Vertraulichkeit dar. Das Mithören von sensiblen Informationen ist auch auf andere Bereiche des elektromagnetischen Spektrums ausweitbar. Der folgende Teil erläutert verschiedene Techniken zur Beeinträchtigung der Informationssicherheit unter Verwendung von Funktechnik.

4.2.3 Abfangen von Funksignalen

In Kombination mit Drohnen kann Funktechnik eingesetzt werden, um Funksignale von bspw. WLAN, DECT oder anderen kabellosen Technologien mitzuschneiden. Ein denkbare Szenario wäre hier der Einsatz von WLAN-Hardware als Nutzlast. Diese kann dann entweder auf dem Gelände des Ziels gelandet, oder im Flug betrieben werden. Mithilfe dieser Hardware können eine Vielzahl von Angriffen auf WLAN durchgeführt werden. Die Plattform Drohne bietet hierbei den Vorteil, dass kabellose Netzwerke erreicht werden können, deren Reichweiten nicht bis an die Grenzen des Firmengeländes reichen. Bewegt man sich rein im Bereich des Abhörens, so kann, mithilfe der Hardware, Netzwerkverkehr mitgeschnitten werden. Bei WLAN kann dieses mitgeschnittene Material, je nach eingesetztem drahtlosen Netzwerkstandard, im Nachgang genutzt werden, um sich Zugang zu gesicherten Netzwerken zu verschaffen [48, 49].

Aber auch andere Funktechnologien können mithilfe adäquater Hardware abgehört werden. In diese Kategorie fallen eine Vielzahl von Protokollen wie Bluetooth, ZigBee, DECT und viele weitere proprietäre Protokolle [50–52]. Ein beispielhafter Typ von Angriff, der in diesem Kontext ein besonders hohes Schadenspotenzial aufweist, ist der auf Funkprotokolle von Peripheriegeräten wie Maus und Tastatur. Eine Art von Angriff dieses Typs sind sogenannte „MouseJack-Angriffe“ [53]. Bereits 2016 belegten Forschende die Verwundbarkeit einer Vielzahl von Funkperipherie. Der Umfang dieses Angriffs fällt hierbei in zwei Kategorien. Bei der ersten Art können, bei erfolgreicher Durchführung, die Tastenanschläge oder Mausbewegungen der jeweils angegriffenen Peripheriegeräte mitgelesen werden. Im Optimalfall können hierdurch sensible Informationen wie Passwörter, persönliche Daten oder vertrauliche geschäftsbezogene Informationen erlangt werden. Dies stellt eine Verletzung der Vertraulichkeit dar. Die zweite Art des Angriffs ist umfangreicher, involviert jedoch auch das Senden von Funksignalen. Angriffe, bei denen Funksignale nicht nur abgehört, sondern auch gesendet werden, werden im nun folgenden Teil näher untersucht.

4.2.4 Senden von Funksignalen

Neben dem Abhören kann die als Zuladung angebrachte Hardware an einer Drohne auch als Sender agieren. Wird die Hardware rein als Sender eingesetzt, so ermöglicht dies etwa das Stören von Funksignalen durch Belegung von Funkkanälen. So könnte unter anderem der Betrieb von WLAN-Netzwerken gestört und ein Betriebsausfall herbeigeführt werden. Ein gezielterer Ansatz ist eine Kombination aus Sender und Empfänger. Durch den gleichzeitigen Einsatz können Man-in-the-Middle-Angriffe wie der Evil-Twin-Angriff bei WLAN durchgeführt werden. Bei erfolgreicher Durchführung

dieses Angriffs verbinden sich Netzwerkteilnehmer durch Verwechslung irrtümlich mit einem WLAN, das unter der Kontrolle von Angreifern steht. Je nach Verschlüsselung des Netzwerkverkehrs kann auch so das Erlangen von sensiblen Informationen erreicht werden, welches wiederum das Schutzziel der Vertraulichkeit verletzt. Da der Fluss des Netzwerkverkehrs in diesem Fall ebenfalls unter der Kontrolle der Angreifer steht, kann auch die Verfügbarkeit eingeschränkt werden.

Auch die zuvor erwähnten MouseJack-Angriffe erhalten durch das Senden von Daten ein erhöhtes Gefahrenpotenzial. Hier wird es in der zweiten Angriffsart bei bestimmten Modellen möglich, selbst Signale zu senden und so effektiv als Peripheriegerät zu agieren. Dies ermöglicht eine Vielzahl weiterer Angriffen wie die Ausleitung von Daten oder das Installieren von Schadsoftware. Je nach hierdurch kompromittiertem System, stellt dies eine Bedrohung für alle drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit dar.

Um weitere Angriffe von Drohnen auf die Informationssicherheit zu identifizieren und die exemplarische Liste von Bedrohungen mit der Expertise der Interviewpartner um praxisnahe Gefahren zu bereichern, werden nun im folgenden Kapitel Experten interviewt.

5 Experteninterviews

Dieser Teil verfolgt das Ziel ein besseres Verständnis der aktuellen Praxislage in Bezug auf die Forschungsfrage zu bekommen. Hierzu wird eingangs erläutert, welche Methoden zur Durchführung und Analyse der Interviews angewandt wurden. Anschließend werden die wesentlichen Gefahren zusammengefasst, welche von Experten während der geführten Interviews genannt wurden. Eine Doppelnennung von Gefahren, welche bereits im Rahmen der Literaturanalyse identifiziert wurden, geschieht nicht. Am Ende des Kapitels werden alle im Rahmen dieser Arbeit identifizierten Gefahren für die Informationssicherheit kompakt in einer Gefahrentabelle dargestellt. Während der Interviews wurden den Experten nebst Fragen zu Gefahren auch allgemeinere Fragen über den Fachbereich sowie Fragen zur Drohnenabwehr gestellt. Diese Ergebnisse fließen maßgeblich in den Teil 7 Abwehrmaßnahmen ein. Auch das Kapitel 8 der Diskussion profitiert von den kritischen Betrachtungsweisen der Experten, welche eine Differenzierung der Gesamtlage ermöglichen.

5.1 Methode

Um verlässliche Ergebnisse aus den Interviews zu ziehen, ist eine sorgfältige Methode während der Durchführung unabdingbar. Dieser Abschnitt gibt den Aufbau des genutzten Fragenkatalogs wieder und geht auf den Hintergrund und das Ziel der jeweiligen Interviewfragen ein. Außerdem wird die Methodik hinter der Analyse der gesprochenen Inhalte erläutert. Den Einstieg in den Abschnitt bildet die Beschreibung des generellen Ablaufs und der Interviewstruktur.

5.1.1 Struktur der Interviews

Um die Reproduzierbarkeit der Ergebnisse sicherzustellen, wurde vor den Interviews ein Fragenkatalog erstellt. Dieser ist im Anhang A der Arbeit beigefügt. Diesen erhielt jeder der Interviewpartner vorab. Zusätzlich zum Katalog erhielt jeder Partner eine Datenschutzerklärung, in der er über die Verwendung seiner Daten aufgeklärt wurde.

Die thematische Struktur des Fragenkatalogs orientierte sich grob an der Struktur dieser Arbeit. So wurden zu Beginn Fragen über Gefahren durch Drohnen auf die Informationssicherheit gestellt, anschließend wurden Möglichkeiten zur Verteidigung diskutiert und letztlich der Fachbereich im Allgemeinen behandelt. Die gewonnenen Erkenntnisse aus der zuvor durchgeführten Literaturrecherche flossen ebenfalls in die Struktur des Katalogs ein. Die Fragen innerhalb des Katalogs sind thematisch offen gestellt. Binäre Fragen wurden weitestgehend vermieden. Diese offene Fragestruktur soll dem Sinn der semistrukturierten Natur der Interviews gerecht werden. Ziel war nicht, quantitative Daten zu erfassen, sondern Fachmeinungen zur Thematik zu

erlangen. Die offene Struktur sollte die Experten anregen, ein breites Spektrum an Themen in Bezug auf die Forschungsfrage anzusprechen. Dies unterstützt die Formulierung von Gegenfragen und beleuchtet damit die Thematik umfassend. Der Hintergrund der Bereiche und Fragen im Fragenkatalog wird im nun folgenden Kapitel näher betrachtet.

5.1.2 Aufbau des Fragenkatalogs

Um einen einfachen Einstieg in das Interview zu ermöglichen sowie eine grundlegende Verbindung zum Interviewpartner aufzubauen, umfasste der erste Teil des Fragenkatalogs eine kurze Vorstellung des Themas, der Forschungsfrage und allen Beteiligten. Diese Vorstellung wurde nicht aufgezeichnet, da keine direkt für diese Arbeit relevanten Inhalte besprochen wurden. Sie sollte dem Interviewpartner das Ziel der Forschung aufzeigen und Vertrauen zwischen Interviewer und Partner aufbauen, um die Qualität der gesagten Inhalte zu erhöhen. Nach der Einführung wurde bei jedem Interview zusätzlich zur schriftlichen, noch die mündliche Zustimmung zur Aufnahme eingeholt.

Das erste Themengebiet behandelte grundlegende Fragen zu Drohnentechnologien. Ziel sollte es hierbei sein, den genauen Kompetenzbereich der Experten zu identifizieren. Außerdem sollte eine Möglichkeit für Rückfragen über Drohnentechnologien, mit denen die jeweiligen Experten gearbeitet haben, geschaffen werden. Ein weiteres Ziel sollte die Erfassung der subjektiven Wahrnehmung von Drohnen sein. Diese Erfassung sollte der neutralen Interpretation der Gesprächsinhalte in der nachfolgenden Analyse der Interviews ermöglichen.

Der nächste thematische Schwerpunkt des Fragenkatalogs lag auf der Identifizierung von Gefahren. Dieser Teil steht in nächster Relation zur Forschungsfrage und soll das Gefahrenpotenzial umgehend beleuchten. Zu Beginn wurden die Experten hierzu um ihre Einschätzung zum Gefahrenpotenzial von Drohnen auf die Informationssicherheit gebeten. Diese Frage sollte eine Reihe von individuellen Gegenfragen zur genaueren Erläuterung und der aktuellen Lage ermöglichen. Anschließend wurden die Experten explizit nach möglichen Gefahren von Drohnen auf die Informationssicherheit gefragt. Bei den Gefahren wurde hierbei nach direkten und indirekten Gefahren unterschieden. Auch hier wurden jeweils Gegenfragen zur genaueren Erläuterung gestellt. Zudem wurden, nach der Erläuterung der Experten, vereinzelt Gefahren aus der Literatur genannt und durch die Meinung der Experten validiert.

Nach den Fragen zum Thema Gefahren wurden die Experten zur Drohnenabwehr befragt. Neben dem primären Ziel, Erkenntnisse über die Drohnenabwehr zu erlangen, stand hier auch die indirekte Identifizierung weiterer Gefahren im Vordergrund. Hierzu wurden die Experten gegen Ende des Themenblocks zu echten Zwischenfällen mit Drohnen aus dem Arbeitsalltag befragt.

Anschließend wurden Fragen zu möglichen Schutzmaßnahmen gestellt. In diesem Teil wurden auch Fragen zu regulatorischen Rahmenbedingungen gestellt, um die Repräsentation der möglichen Gefahrenlage in der Realität zu erfassen.

Den Abschluss des Katalogs bildete die Befragung zum Ausblick und der weiteren Entwicklung der Forschungsfrage. Den Einstieg zu weiteren Gegenfragen bot hierbei eine Frage zur aktuellen und künftigen Lage der Gefahren von Drohnen auf die Informationssicherheit. Abschließend wurden die wesentlichen Inhalte des Interviews noch einmal kurz zusammengefasst. Diese Zusammenfassung diente dem Vorbeugen von Missverständnissen und der Vollständigkeit, da es den Experten erlaubte, erwähnenswerte Inhalte hinzuzufügen. Nach der Durchführung der Interviews wurden die gesprochenen Inhalte analysiert. Die Herangehensweise bei der Analyse dieser Inhalte, sowie der allgemeinen Inhalte der Interviews, wird nun im folgenden Abschnitt betrachtet.

5.1.3 Analyse des Inhalts

Nach der Durchführung der Interviews wurden die Inhalte analysiert, um die wesentlichen Forschungsergebnisse darzustellen. Zur Analyse der Inhalte wurde die Methode der qualitativen Inhaltsanalyse, wie in [54] von Mayring beschrieben, angewendet. Diese eignet sich für jegliche Art von zwischenmenschlicher Kommunikation, jedoch insbesondere für Experteninterviews. Vorteil dieser Methodik ist die Reliabilität und Validität der Ergebnisse. Um eine korrekte qualitative Inhaltsanalyse durchzuführen, folgt diese Arbeit der Vorgehensweise nach Mayring.

Mayring beschreibt hierzu schrittweise, wie die Analyse durchgeführt wird. Hierzu wird zu Beginn das Material festgelegt, welches analysiert werden soll. Im Fall dieser Arbeit besteht dies aus Aufzeichnungen von geführten Online-Interviews.

Der zweite Schritt nach Mayring ist die Analyse der Entstehungssituation. Hier sollen die Motive und Ziele bei der Entstehung des Materials erörtert werden. Da das zu analysierende Material im Rahmen dieser Forschung entstanden ist, steht das Motiv und Ziel im Einklang mit der Forschungsfrage dieser Arbeit. Weitere Motive können auch dem Unterkapitel 5.1.2 über den Aufbau des Fragenkatalogs entnommen

werden. Außerdem soll der Kontext des Materials erläutert werden. Hierzu zählt bspw. der Hintergrund der Interviewpartner oder die Entstehungssituation. Diese Informationen wurden bereits im Unterkapitel 5.1.1 über die Struktur der Interviews genannt.

Im dritten Schritt werden die formalen Charakteristika des Materials festgelegt. Dies beschreibt also, in welcher Form das Material vorliegt. Um die Interviews mithilfe der Technik Mayrings analysieren zu können, wurden diese transkribiert. Das Material für diese Arbeit liegt also in Textform vor.

Im darauffolgenden Teil wird festgelegt, in welche Richtung das Material analysiert wird. Diese kann je nach Feld der Forschung unterschiedlich sein. Da es bei dieser Arbeit um die objektive Erfassung der Gefahrenlage geht, trägt eine Untersuchung der Wirkung des Textes auf die Zielgruppe oder eine Untersuchung des soziokulturellen Hintergrundes der Interviewpartner wenig zur Beantwortung der Forschungsfrage bei. Diese Informationen fließen in Form des Kontexts in diese Untersuchung ein. Die Richtung der Analyse in dieser Arbeit ist der im Interview behandelte Gegenstand in Form der Interviewfragen.

Anschließend soll die Fragestellung theoriegeleitet differenziert werden. Dies bedeutet die Einordnung des Materials in den Kontext der theoretischen Ausgangssituation. Die Einordnung der Forschungsfrage in den wissenschaftlichen Konkurs ist im Kapitel 3 dargestellt.

Im letzten Teil der Vorgehensweise nach Mayring muss eine passende Analysetechnik gewählt werden. Hierbei beschreibt Mayring die Ansätze deduktiv, induktiv und explikativ. Diese Arbeit wählt den induktiven Ansatz. Dieser eignet sich vorrangig für explorative Inhalte, während die anderen Ansätze Vorteile für andere Arten der Forschung bieten. Bei der induktiven Analyse werden die wesentlichen Aussagen des Materials inhaltlich sukzessive zusammengefasst und in Kategorien gegliedert. Die Bildung der Kategorien erfolgt dabei während der Analyse. Die erstellten Kategorien während der Analyse des Inhalts sind in Form des Kodierleitfadens im Anhang C dieser Arbeit angehängt. Die Ergebnisse der Inhaltsanalyse werden im weiteren Verlauf dieses Kapitels dargestellt.

Nach der Erläuterung der methodischen Grundlagen für die Experteninterviews werden nun die Ergebnisse der Interviews dargestellt. Hierzu wird der Kontext der Ergebnisse zu Beginn des nächsten Abschnitts mit der Methodik bei der Auswahl der Interviewpartner bereichert.

5.2 Ergebnisse der Experteninterviews

Bei der Durchführung der Interviews ist es wichtig, auf die Auswahl der Interviewpartner zu achten. Alle Interviewpartner sollten mit der Materie vertraut sein und Erfahrungen in den Bereichen Drohnen und Informationssicherheit gemacht haben. Im Rahmen dieser Arbeit wurden Interviews mit Partnern aus verschiedenen Fachbereichen durchgeführt. Die folgende Tabelle 2 zeigt die Branchen, Tätigkeitsfelder der Interviewpartner sowie die jeweilige Interviewlänge in Minuten.

ID	Branche	Tätigkeitsfeld	Dauer
I1	Pharmaindustrie	Werkssicherheit	56:08
I2	Pharmaindustrie	Werkssicherheit	36:38
I3	Forschung	Projektleitung Drohnenabwehr	36:33
I4	Unternehmensberatung	Cybersicherheit und Datenschutz	29:41
I5	Behörde	Technischer Berater	47:01
I6	Dienstleistung	Vermessung	47:39

Tabelle 2: Übersicht der Interviewpartner sowie deren fachliches Umfeld

Während des Interviews bietet sich ein nicht standardisiertes, semistrukturiertes Vorgehen an. Die zu sammelnden Daten sollen sich hierbei anhand einer thematischen Struktur orientieren. Dieser Ansatz fördert ein offenes Gespräch mit den Partnern. Es weist daher eine hohe Flexibilität bei der Datenerhebung auf, da neue Fragen basierend auf den Antworten der Partner gestellt werden können. Diese Flexibilität eignet sich daher gut bei der Exploration des Gebietes der Forschungsfrage.

Die Durchführung der Interviews selbst erfolgte jeweils in Form von Online-Video-Meetings. Die gesprochenen Inhalte wurden, nach Einverständnis der Partner, aufgezeichnet und im Nachgang zu Analyse Zwecken transkribiert.

Nach der Analyse der Inhalte konnten zwei wesentliche Kategorien von Gefahren, welche von den Experten identifiziert wurden, erstellt werden. Bedrohungen der ersten Kategorie werden nun im folgenden Abschnitt erläutert.

5.2.1 Kameratechnik

Ein Großteil der interviewten Experten identifizierte Kameratechnik an Drohnen als eine der größten Gefahren für die Informationssicherheit. Um der Informationssicherheit abzutragen, muss hierzu nicht immer spezialisierte Kameratechnik verwendet werden. So sagt I1 *„auch mit einer schlechten Kamera kann ich oft aufgrund der hohen Nähe, mit der ich ran fliegen kann, relativ viel Schaden anrichten“* (I1, Pos. 23).

I1 betont auch, dass diese Brisanz durch Einsatz von Kameraaufhängungen und leistungsstarken Kameras noch mehr an Bedeutung gewinnt. Diese Art von Angriff wurde auch bereits im Rahmen der Literaturanalyse identifiziert.

Der Schaden in diesem Fall kann nicht nur in Form von Informationsabfluss geschehen. Auch das Generieren von tagesaktuellen Bildern oder Bewegungsprofilen kann laut I2 eine Gefahr darstellen. I2 weist darauf hin, dass das Erstellen von Bewegungsprofilen aufgrund der meist eingebauten GPS-Funktion auch einfach auf Lieferketten übertragen werden könnte. Diese Informationen können als vorbereitende Maßnahme für weitere Angriffe genutzt werden.

Eine weitere vorbereitende Maßnahme ist das Ausspähen von Gerätetypen. So identifiziert I4 hierzu folgendes Szenario: *„Wenn ich zum Beispiel wissen will, wo die entsprechenden Sicherheitskameras sind oder welche Marke die Sicherheitskameras haben, um sie dann im zweiten Schritt über einen Netzwerkangriff unschädlich zu machen.“* (I4, Pos. 14). Dieses Szenario lässt sich von den beispielhaften Sicherheitskameras auf jegliche technische Einrichtung im Außenbereich ausweiten. So könnten Typ-Informationen über das eingesetzte Zugangskontrollsystem vorteilhaft für einen späteren Angriff sein. Diese Art von Bedrohung wurde während der Literaturanalyse bisher nicht identifiziert. Zusammen mit der vorher genannten Möglichkeit zur Aufklärung von Lieferketten oder Bewegungsprofilen erhält diese Bedrohung den Eintrag „Aufklären von Unternehmensressource“ in der Gefahrentabelle (Tabelle 3) am Ende dieses Kapitels. Der geschätzte direkte Schaden sollte hierbei gering ausfallen. Angriffe, die durch diesen begünstigt oder ermöglicht wurden, können jedoch einen sehr hohen Schadenswert aufweisen.

Der Einsatz von Drohnen zu Zwecken der Industriespionage wurde jeweils von I3 - I5 unabhängig genannt. *„Ja, ich glaube, das Klassiker Beispiel sind immer irgendwelche Prototypen von Autoherstellern, wo man dann versucht, Fotos davon zu machen.“* (I4, Pos. 6). Diese Art der Kompromittierung der Informationssicherheit muss sich auch hierbei nicht auf die Automobilindustrie beschränken. Die Ziele könnten auch Forschungseinrichtungen oder jegliche Organisation mit offenem Betriebsgelände sein. Die erlangten Informationen sind hierbei eher physischer Natur und beschränken sich nicht auf Dokumente oder Passwörter.

Neben dem Einsatz an der Drohne selbst, wäre laut I1 und I2 auch das Verbringen von Kameras mithilfe von Drohnen ein mögliches Szenario. *„[Es gibt] Superkleber, die recht schnell kleben und dann eine Kamera dran hängt, die dann ans Fenster gedockt wird“* (I2, Pos. 10). Je nach Platzierung und Größe der Kamera könnten so

Innenräume über mehrere Tage hinweg überwacht werden. I1 und I2 erwähnen in diesem Kontext außerdem, dass diese Art von Angriff bei Nacht ausgeführt werden können, um das Entdeckungsrisiko während der Platzierung zu minimieren.

5.2.2 Funktechnik

Eine weitere Art von Zuladung, die von der Mehrheit der Interviewten genannt wurde, ist der Einsatz von Funktechnik. Die Art der Angriffe ist hierbei vielfältig.

Das Sammeln von Informationen im Zusammenhang mit WLAN wurde von I2, I4 und I5 als mögliche Bedrohung identifiziert. *„Dann stelle ich meine Drohne aufs Dach, mache die aus und habe [...] das System genau vor Ort [...] ich komme natürlich dann nicht physikalisch rein ins Netz, aber alles, was schnurlos wireless Angriffsmethoden sind, das kann ich natürlich damit machen.“* (I5, Pos. 111). Der Angriff mittels Bluetooth ist ebenfalls ein mögliches Szenario. I4 berichtet hierbei von einem in einer Laborumgebung durchgeführten Angriff auf einen vernetzten Roboterarmes mithilfe einer Drohne.

Aber auch der Angriffe anderer Frequenzen und Funkprotokolle sind möglich. I3 nennt hierfür LoRaWAN oder Mobilfunk. I5 berichtet von einem Konzept für einen Denial of Service Angriff auf das Mobilfunknetz mobiler Endgeräte. Hierbei würde ein Software Defined Radio als Zuladung an eine Drohne befestigt. Dieses agiert dann als mobile Basisstation. Sie wird so konfiguriert, dass sie, sobald sich ein Endgerät mit ihr verbindet, die Verbindung ablehnt. Diese Ablehnung erfolgt unter Nutzung bestimmter Gründe zur Abweisung. Diese führen dem Mobilfunkstandard zufolge dazu, dass das Endgerät bis zum Neustart keine weiteren Verbindungsversuche mit dem Mobilfunknetz unternimmt. Die Unterbrechung der mobilen Konnektivität bietet eine Vielzahl von Möglichkeiten für Angreifer.

Als weiteres Beispiel nennt I5 für die Unterdrückung von Alarmmeldungen einer Alarmanlage das folgende Szenario: *„[Hypothetisch fliegt man] mit einer Drohne hin und [legt] dann [...] eine metallisierte Rettungsdecke [...] [über eine Richtfunkantennen] drüber. Da gehen ganze Basisstationen, gehen in die Knie“* (I5, Pos. 122). Neben diesem physischen Angriff hebt I4 noch den Einsatz von Jammern zum Blockieren von Frequenzen hervor.

Um eine kompakte Betrachtungsweise der in dieser Arbeit identifizierten Gefahren zu ermöglichen, werden nun im folgenden Teil alle Gefahren klassifiziert und anschließend in einer Gefahrentabelle dargestellt.

5.3 Klassifizierung

Für die Klassifizierung bieten sich verschiedene Arten der Unterscheidung an. Zum einen könnten Gefahren nach Technik eingeordnet werden. Hier wäre etwa eine Gruppierung aller Angriffe, welche den Einsatz vonameratechnik erfordern, möglich. Diese Art der Klassifizierung würde die Identifizierung gefährdeter Fachbereiche ermöglichen. Der zweite Ansatz ist die Klassifizierung in primäre und sekundäre Gefahren. Primäre Gefahren stellen hierbei Angriffe dar, durch welche Angreifer nach erfolgreicher Durchführung die Informationssicherheit signifikant verletzen, ohne weitere Maßnahmen ergreifen zu müssen. Ein Beispiel hierfür wäre das Mitlesen sensibler Information mithilfe einer Drohne. Bei sekundären Gefahren werden nachfolgende Angriffe durch den Gewinn von Information erleichtert. Beispiel dafür ist das von I4 genannte Ausspähen von Systemen wie Überwachungskameras, welche dann gezielt angegriffen werden können. Diese Einteilung ermöglicht eine verbesserte Risikobetrachtung, da primäre Gefahren aufgrund der fehlenden Notwendigkeit eines zweiten Angriffs im Allgemeinen ein höheres Schadenspotenzial darstellen. Außerdem trägt diese Klassifizierung dazu bei, eine verständliche Übersicht der Bedrohungen, auch für weniger technisch versierte Lesende, sicherzustellen. Diese Arbeit wählt zur Darstellung einen hybriden Ansatz, wobei die Bedrohungen nach Kategorie und nach Technologie gruppiert werden. Die folgende Abbildung 7 zeigt diese gruppierte Übersicht der Bedrohungen.

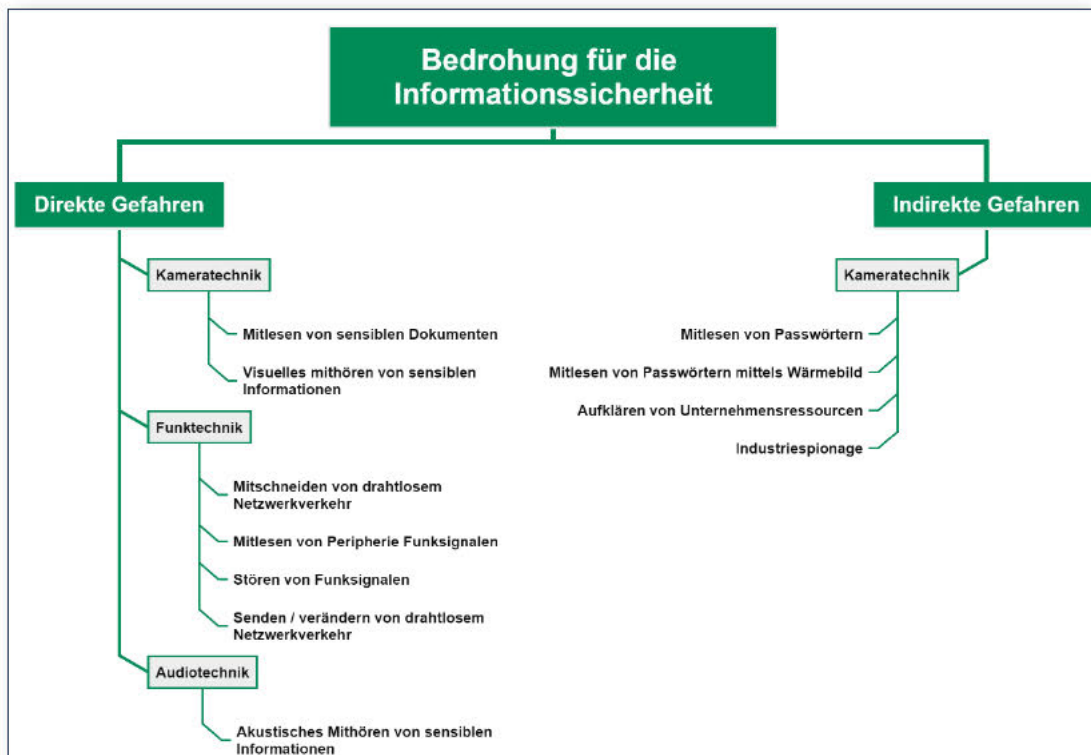


Abbildung 7: Klassifizierte Bedrohungen

Zusätzlich zur Klassifizierung werden alle Gefahren zu Zwecken der Übersichtlichkeit noch einmal in der unten stehenden Gefahren-Tabelle 3 aufgeführt. Sie erhalten zusätzlich die geschätzten Metriken Kosten zur Durchführung, geschätzter wirtschaftlicher Schaden am Ziel des Angriffs sowie technische Komplexität zur Durchführung. Außerdem wird das Maß der Beeinträchtigung der Informationssicherheit in Form der eingangs erläuterten Modelle CIA und STRIDE für jede Bedrohung angegeben. Diese Einordnung bezieht sich bei indirekten Angriffen auf das maximale anzunehmende Schadenspotenzial, welches mit den erlangten Informationen möglich ist. Die Klassifizierung der Gefahr ist ebenfalls aufgeführt. Um die Realitätsnähe der angegebenen Metriken sicherzustellen, orientieren sich diese überwiegend an den offiziellen Vorgaben des BSI-Standard 100-4 [55]. Die geschätzten Kosten werden in die Kategorien „Gering“ (0 € – 1000 €), „Mittel“ (1000 € - 10.000 €) und „Hoch“ (Über 10.000 €) eingeteilt. Da bei diesen Angriffen der Preis für Hardware nicht inbegriffen ist, wird pauschal ein Preis von 450 € addiert. Dieser Preis orientiert sich am Verkaufspreis der Hardware einer selbst gebauten Drohne inkl. GPS-Empfänger für die automatische Navigation [56]. Der geschätzte Schaden unterteilt sich gemäß dem Standard in „niedrig“ (kaum spürbare Auswirkungen), „normal“ (spürbare Auswirkungen), „hoch“ (erhebliche Auswirkungen) und „sehr hoch“ (Auswirkungen existenziell bedrohlich). Die technische Komplexität unterteilt sich ebenfalls in drei selbst gebildete Kategorien. Niedrig ist die Komplexität eines Angriffs, wenn zum Durchführen keine spezialisierte Software nötig ist und die nötige Hardware einfach verfügbar ist. Angriffe mit mittlerer Komplexität nutzen frei verfügbare Software oder einfache, selbst geschriebene Skripte sowie Hardware, welche weiteren Zusammenbau benötigt. Eine hohe Angriffskomplexität ist gegeben, wenn die eingesetzte Software selbst entwickelt werden muss oder selbst konstruierte Drohnen mit spezialisierter Hardware eingesetzt werden.

Die Gefahren-Tabelle setzt außerdem ein Ampelsystem ein, um Lesenden eine schnelle Einordnung der Bedrohungen zu ermöglichen. Dieses gibt an, wie der Wert der jeweiligen Metrik das Gefahrenpotenzial beeinflusst. Die Abstufung dieser Ampel ist in der folgenden Abbildung dargestellt.

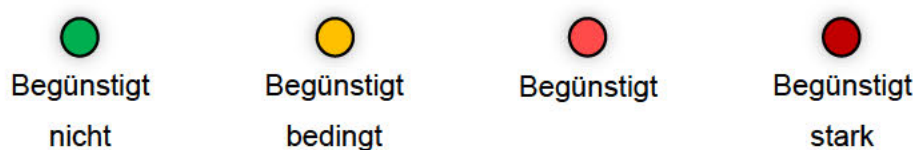


Abbildung 8: Ampelsystem Gefahrentabelle

Bedrohung	Geschätzte Kosten	Geschätzter Schaden	Technische Komplexität	Klassifizierung	Bedrohte Schutzziele
Mitlesen von Passwörtern	Mittel	Mittel – Sehr hoch	Niedrig	Indirekt	C, I, A T, R, I, D, E
Mitlesen von Passwörtern mittels Wärmebild	Mittel – Hoch	Mittel – Sehr hoch	Mittel	Indirekt	C, I, A T, R, I, D, E
Mitlesen von sensiblen Dokumenten	Gering – Mittel	Niedrig – Sehr hoch	Mittel – Niedrig	Direkt	C I
Akustisches Mithören von sensiblen Informationen	Gering	Mittel – Sehr hoch	Mittel – Niedrig	Direkt	C I
Visuelles mithören von sensiblen Informationen	Gering – Mittel	Niedrig – Sehr hoch	Niedrig	Direkt	C I
Mitschneiden von drahtlosem Netzwerkverkehr	Gering	Niedrig – Sehr hoch	Mittel	Direkt	C I, E
Mitlesen von Peripherie Funksignalen	Gering	Niedrig – Sehr hoch	Mittel	Direkt	C I, E
Stören von Funksignalen	Mittel	Niedrig – Sehr hoch	Niedrig	Direkt	A D
Senden / verändern von drahtlosem Netzwerkverkehr	Mittel	Niedrig – Sehr hoch	Mittel – Niedrig	Direkt	C, I, A S, T, R, I, D, E
Aufklären von Unternehmensressourcen	Niedrig	Niedrig	Niedrig	Indirekt	C I, E
Industriespionage	Niedrig	Niedrig – Sehr hoch	Niedrig	Indirekt	C I

Tabelle 3: Gefahrentabelle aller Gefahren

6 Praktischer Versuch

In diesem Teil soll eine der in 4.2 identifizierten Gefahren in der Praxis durchgeführt werden. Dies soll die Machbarkeit von Drohnenangriffen belegen. Basierend auf den Faktoren Kosten, Schaden und technischer Komplexität aus den Gefahren-Tabellen, wählt diese Arbeit die Gefahr „Mitlesen von sensiblen Dokumenten“. Zu Beginn wird hierzu erst Ziel und Konzept dieses Versuchs erläutert, anschließend wird die Methodik während des Versuchs beschrieben. Der letzte Teil des Kapitels bietet die Darstellung der Gegebenheiten während des praktischen Versuchs sowie die indessen gewonnenen Ergebnisse.

6.1 Ziel und Konzept

Ziel des Versuchs soll es sein, mithilfe einer an einer kommerziellen Drohne befestigten Kamera, sensible Informationen zu erlangen. Die Informationen können in vielen Formen, wie ausliegenden Dokumenten oder Bildschirmhalten, vorliegen. Aber auch physische Gegebenheiten wie offenstehende Prototypen im Außenbereich können sensible Informationen für Unternehmen sein.

Mit der Durchführung des Versuchs sollen eine Reihe von Kernfragen beantwortet werden. Zu Beginn soll überprüft werden, ob das heimliche Erfassen von sensiblen Informationen durch Drohnen technisch umsetzbar ist. Dieses Ziel ist erreicht, wenn es den Durchführenden möglich ist, anhand der erfassten visuellen Signale, relevante Informationen auszulesen. Die Informationen beschränken sich bei diesem Versuch auf die Formen Bildschirminhalt und offenliegendes Dokument. Der Einsatz von Künstlicher Intelligenz zur Unterstützung in diesem Prozess ist aufgrund möglicher falscher Ergebnisse nicht Teil des Versuchs. Es ist jedoch erwähnenswert, dass es bereits Forschung zum Thema der Extraktion von Informationen aus schwer leserlichem Text, wie [57, 58], gibt, welche den Ergebnissen dieses Versuchs zusätzliche Brisanz verleihen könnten.

Des Weiteren soll die Entdeckungswahrscheinlichkeit eines solchen Angriffs untersucht werden. Diese Kernfrage soll die Viabilität des Angriffs in der Realität belegen. Um die Praxistauglichkeit sicherzustellen, muss der Angriff mindestens einmal von Probanden unbemerkt durchgeführt werden.

Die letzte Kernfrage soll erfassen, welche Abwehrmaßnahmen gegen derartige Angriffe eingesetzt werden können. Im Rahmen des Versuches soll die Effektivität von Sichtschutzmaßnahmen in Form von Sichtschutzfolien untersucht werden.

Anhand dieser Kernfragen lässt sich der Versuchsaufbau formulieren. Um das Maß der Lesbarkeit bewerten zu können, werden fiktive sensible Daten in Form von kurzen Sätzen generiert. Das hierbei genutzte Referenzblatt ist im Anhang D anbei. Diese Sätze werden dann auf einem Bildschirm dargestellt. Jeder Satz erhält eine andere Schriftgröße. Hierbei wird darauf geachtet, dass die Dimensionen bei der Darstellung der einzelnen Sätze, während jedem Versuchsaufbau, konsistent sind. Für die Inhalte in Form von offenliegenden Dokumenten wird ein zweites Exemplar der Beispieldaten ausgedruckt und in der Nähe des Monitors ausgelegt, um einen Arbeitsplatz zu simulieren. Ein Versuchsteilnehmer wird dann vor den Monitor gesetzt. Er erhält eine Aufgabe in Form eines Fragebogens, welcher Büroarbeit simulieren soll. Der simulierte Arbeitsplatz befindet sich für diesen Versuch immer in der Nähe eines Fensters. Die Ausrichtung des Arbeitsplatzes ist orthogonal zum Fenster.

Zur Durchführung platzieren sich die Durchführenden mit ausreichend Abstand zum Fenster des Probanden. Nach einer zufälligen Zeit starten sie die Drohne mit der befestigten Kamera. Sie versuchen sich nun unerkannt dem Fenster des Probanden zu nähern und die sensiblen Informationen auszulesen. Die Videosignale werden hierbei für eine spätere Analyse aufgezeichnet. Sobald der Proband die Drohne bemerkt oder genug Aufnahmen durch die Durchführenden generiert wurde, ist der Versuch beendet. Die Angreifer probieren jetzt anhand des aufgenommenen Bildmaterials die sensiblen Daten auszulesen.

Um die Effektivität einer Abwehrmaßnahme in diesem Szenario zu bewerten, wird der Versuch erneut durchgeführt. Zuvor wurde das Fenster des Probanden jedoch mit einer Sichtschutzfolie ausgestattet. Die Ergebnisse werden, wie im Versuch zuvor auch, erfasst.

Wie diese Methodik während des Versuches in der Realität umgesetzt und durchgeführt wurde, wird im nun folgenden Unterkapitel beschrieben.

6.2 Durchführung

Der Versuch setzt eine, auf die Kernfragen ausgerichtete, Methodik ein. Hierbei wird darauf geachtet, dass die Ergebnisse möglichst wiederholbar und reliabel sind. Um dies zu erreichen, soll der Einfluss von subjektiven sowie Umgebungsfaktoren mit vertretbarem Aufwand möglichst reduziert werden. Der Versuch wird daher mit verschiedenen Probanden zu verschiedenen Tageszeiten durchgeführt. Die Wiederholung des Versuches zu verschiedenen Jahreszeiten und an verschiedenen Lokationen ist aufgrund des zeitlichen Rahmens nicht Teil der Versuchsmethodik.

6.2.1 Rahmenbedingungen

Alle Versuche wurden an der gleichen Lokation mit einem einheitlichen Versuchsaufbau durchgeführt. Der Aufbau des Versuches ist auf der folgenden Abbildung 9 dargestellt.

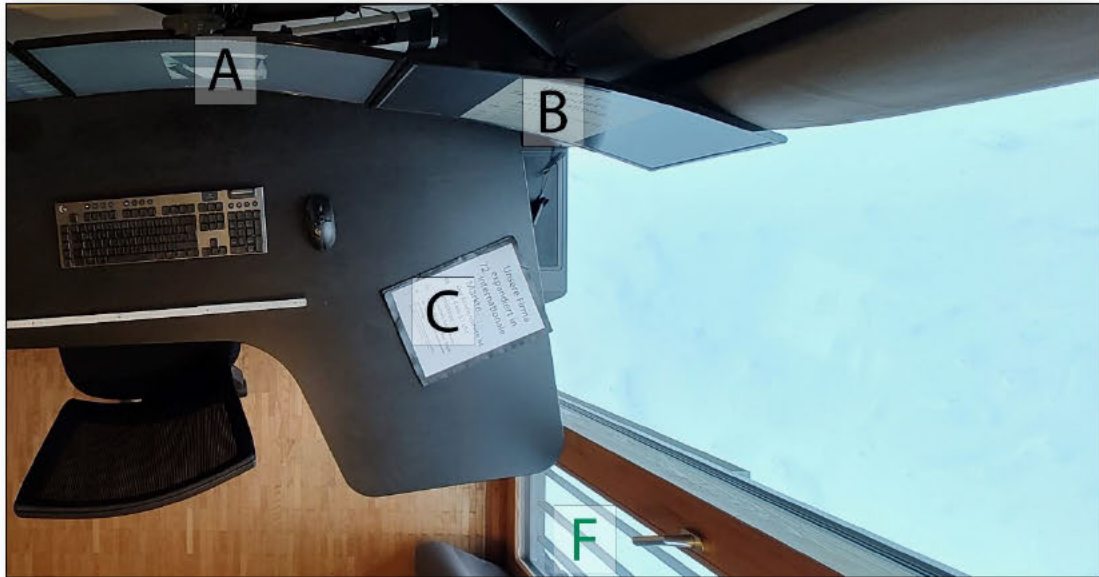


Abbildung 9: Versuchsaufbau Innenansicht

Der Versuchsaufbau zeigt insbesondere die Monitore A und B sowie das Dokument C. Die Monitore haben jeweils eine Größe von 27 Zoll (ca. 69 cm) und einer Auflösung von 1080p. Monitor B zeigte das Dokument mit einer Skalierung von 100 % mithilfe des Textverarbeitungsprogrammes Microsoft Word. Das gedruckte Dokument lag in der Formatgröße DIN A4 vor. Im Rahmen des Versuches wurde der Monitor A von den Probanden für die Durchführung des Fragebogens verwendet. Monitor B zeigte während der Durchführung aller Experimente das sensible Testdokument mit den fiktiven Daten an. Diese Daten liegen zusätzlich in gedruckter Form als Dokument C aus. Die Aufnahmen des Monitors B sowie des Dokumentes C geschahen durch das in der Abbildung unten rechts abgebildete Fenster F. Dieses Fenster ist auch auf der folgenden Abbildung 10: Versuch Außenansicht und Flugpfade zu erkennen.



Abbildung 10: Versuch Außenansicht und Flugpfade

Neben dem Fenster F und den Flugpfaden P 1 - 3, welche in den folgenden Kapiteln relevant werden, zeigt Abbildung 10 auch die klimatischen Gegebenheiten. So waren während der Versuche jeweils leichter Schneefall und eine Schneedecke von 60 bis 80 Zentimetern zu verzeichnen. Der Himmel war stets bedeckt, ohne direkte Sonneneinstrahlung auf das Fenster. Die Zeiten, zu denen die Flüge durchgeführt wurden, lagen jeweils zwischen 13:00 Uhr mittags und 18:00 Uhr abends.

Technisch wurden für den Versuch zwei verschiedene Drohnenmodelle der Firma DJI eingesetzt. Das erste Modell, die Mavic Pro, erschien im Jahre 2016 und besitzt eine schwenkbare Kamera mit einer Auflösung von 12,35 Megapixel [59]. Die zweite Drohne, Mavic 2 Mini, besitzt eine vergleichbare Auflösung von 12 Megapixel [60] und erschien 2020. Die eingesetzten Drohnenmodelle sind auf der folgenden Abbildung 11 dargestellt.



Abbildung 11: Während des Versuchs eingesetzte Drohnen

6.2.2 Kernfrage Machbarkeit

Um die Machbarkeit des Angriffs festzustellen, wurden Bild- und Videoaufnahmen aus verschiedenen Perspektiven sowohl von Monitor B als auch von Dokument C erstellt. Die verschiedenen Perspektiven sind auf Abbildung 10 zu sehen. Hierbei zielen P1 und P3 auf das Erlangen von Informationen aus dem ausgedruckten Dokument C ab. P2 soll den Inhalt des Monitors B erfassen. Das Material wurde nach der Erfassung analysiert und mithilfe von Bildbearbeitungsprogrammen verbessert. Insbesondere wurden Korrekturen in Bezug auf Kontrast und Perspektive vorgenommen, um die Leserlichkeit des Textes zu verbessern. Die verbesserten Ergebnisse sind untenstehend auf Abbildung 12 und Abbildung 13 zu sehen.



Abbildung 12: Verbesserte Ergebnisse des Dokuments



PB1



PB2



PB3



PB4

Abbildung 13: Verbesserte Ergebnisse des Monitors

Wie vor allem auf PB1 und PC1 zu sehen ist, sind Informationen bis zum Schriftgrad 28 deutlich lesbar. Die Inhalte in den Schriftgraden 16, 13 und 12 sind aufgrund mangelnder Auflösung aus den Aufnahmen nicht bestimmbar. Die Machbarkeit des Angriffs lässt sich daher bedingt feststellen, da die Inhalte gelesen werden können, jedoch nur mit ausreichender Schriftgröße.

Es gilt jedoch zu beachten, dass die eingesetzten Drohnen dem Stand der Technik im Jahre 2016 entsprechen. Aktuelle Modelle wie die DJI Mavic 3 Classic (Marktstart 2021) bieten eine Auflösung von 20 Megapixel [61]. Höherwertige Modelle wie die DJI Mavic 3 Pro (Marktstart 2023) besitzen zusätzlich Telekameras mit einem verlustfreien optischen Vergrößerungsfaktor von bis zu sieben bei einer Auflösung von zwölf Megapixeln [5]. Auch der Einsatz von externen Kameras als Zuladung zu der Drohne

ist denkbar. So kann die eingesetzte Mavic Pro Drohne eine Zuladung von bis zu knapp einem Kilo tragen [62]. Damit wäre es möglich, auch handelsübliche Smartphones mit höher auflösenden Kameras zu verbringen.

Um ungefähren Vergleich mit dem aktuellen Stand der Technik der aktuellen Drohnen zu ziehen, wurden Bilder des Fensters F mit einer herkömmlichen Digitalkamera aufgenommen. Die genutzte Kamera besitzt eine Auflösung und 20,3 Megapixeln bei einer Brennweite von 24 mm. Dies entspricht ungefähr den Ergebnissen eines aktuellen Modells wie der DJI Mavic 3 [61], welche eine Auflösung von 20 Megapixel bei gleicher Brennweite hat. Die folgende Abbildung 14 stellt das Ergebnis mit einer solchen Kamera dar.

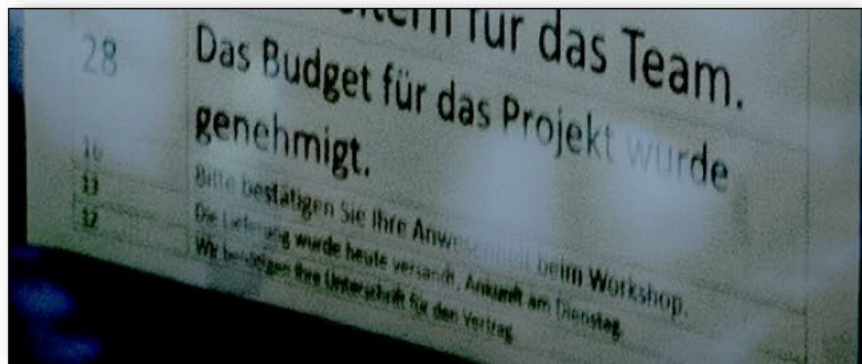


Abbildung 14: Vergleichsaufnahme mit höherer Auflösung

Mit einer höheren Auflösung wird auch Text in kleineren Schriftgrößen lesbar. So sind die sensiblen Informationen auch bis zum Schriftgrad 12 lesbar. Die Machbarkeit und das Gefahrenpotenzial des untersuchten Angriffs erhalten also mit dem Einsatz aktueller Drohnen einen höheren Stellenwert.

Wie auf Abbildung 14 sowie auf den Teilen PB1 und PB2 der Abbildung 13 zu sehen ist, spielen Reflexionen der Fensterscheibe während der Erfassung der sensiblen Informationen ebenfalls eine Rolle. Die Kameratechnik bietet zur Minimierung von Reflexionen spezielle Polarisationsfilter, welche das reflektierte Licht herausfiltern sollen. Im Rahmen des Versuchs wurde ein solcher Filter bei jeder Durchführung angebracht. Jedoch konnte aufgrund der Bauweise des Fensters die Reflexion nur minimal verringert werden. Auch das Anbringen eines Polarisationsfilters während der Vergleichsaufnahme brachte keinen nennenswerten Mehrwert bei der Erfassung der Informationen. Zusätzlich ist zu beachten, dass der Einsatz von Polarisationsfiltern auch, je nach Bauform, das vom Bildschirm emittierte Licht filtern könnte. Die wetterlichen Gegebenheiten während des Versuchs begünstigten die Entstehung von Reflexionen in der Fensterscheibe durch die geschlossene Schneedecke. Bei der

Wiederholung des Versuchs in reflektionsärmeren Umgebungen könnten andere Ergebnisse entstehen.

Das untersuchte Szenario setzt voraus, dass sensible Dokumente in der Nähe des Fensters sichtbar sind. Mit dieser Voraussetzung kann auch davon ausgegangen werden, dass sich ein Mitarbeiter in der Nähe dieser Dokumente befindet. Da Drohnen ein signifikantes Fluggeräusch vorweisen, besteht das Risiko, dass der Mitarbeiter die Drohne entdeckt. Um die Durchführbarkeit des Angriffs in der Realität abschätzen zu können, soll nun im folgenden Experiment mit der Beantwortung der zweiten Kernfrage das Entdeckungsrisiko durch Mitarbeiter untersucht werden.

6.2.3 Kernfrage Entdeckungsrisiko

Zur Beantwortung der zweiten Kernfrage wurde der gleiche Versuchsaufbau wie in der obenstehenden Abbildung 9 genutzt. Insgesamt wurde der Versuch mit fünf Probanden durchgeführt. Um ein möglichst praxisnahes Ergebnis zu erhalten, sollte die Unbefangenheit der Probanden maximiert werden. Hierzu wurden die Probanden zu Beginn des Versuchs nicht über das tatsächliche Ziel der Forschung aufgeklärt. Stattdessen wurde den Probanden das Ziel genannt, die Expertise der allgemeinen Bevölkerung durch die Beantwortung von Fragen zum Thema Drohnen zu erfassen. Da die Fragen nicht direkt in die Forschung einfließen, wurden diese mithilfe einer Sprach-KI generiert. Diese Fragen sind im Anhang E : Exemplarische Versuchsfragen aufgeführt. Um ein Büroumfeld zu simulieren, wurden während der Durchführung beispielhaft Hintergrundgeräusche eines Büros über einen Lautsprecher abgespielt. Im Ausgangszustand lag die Lärmbelastung am Sitzplatz der Probanden bei ca. 40 Dezibel. Das Fenster war während des gesamten Versuchs geschlossen. Während die Teilnehmenden die Fragen beantworteten, probierten die Durchführenden, mit Hilfe der Drohne über die verschiedenen Perspektiven P1 - 3 (s.a. Abbildung 10) sensible Daten zu erlangen. Im Laufe der Versuche ergaben sich bei den Versuchspartnern (VPs) folgende Ergebnisse, welche in der folgenden Tabelle 4 dargestellt sind.

ID	Flugpfad bei Entdeckung	Durchführungszeitpunkt
VP1	P3	Tag
VP2	P3	Tag
VP3	-	Abend
VP4	P3	Abend
VP5	-	Tag

Tabelle 4: Ergebnisse Entdeckungsrisiko

Aus den Ergebnissen der Tabelle lässt sich ein allgemein niedriges Entdeckungsrisiko ableiten. So entdeckten nur drei der fünf Teilnehmer die Drohne. Zuvor konnte die Drohne bereits vor ihrer Entdeckung sensible Informationen aus den Perspektiven P1 und P2 erfassen. Alle Teilnehmer, welche die Drohne entdecken, gaben an, dass sie die Drohne durch Blickkontakt entdeckten. Keiner der Teilnehmer entdeckte die Drohne anhand des Fluggeräusches. Dies lässt sich vorrangig auf die geringe Geräuschentwicklung zurückführen. Bei geschlossenem Fenster konnte bei einer Messung des Geräuschpegels kein signifikanter Unterschied während dem Flug der Drohne festgestellt werden. Der einzige andere Entdeckungsweg ist der visuelle.

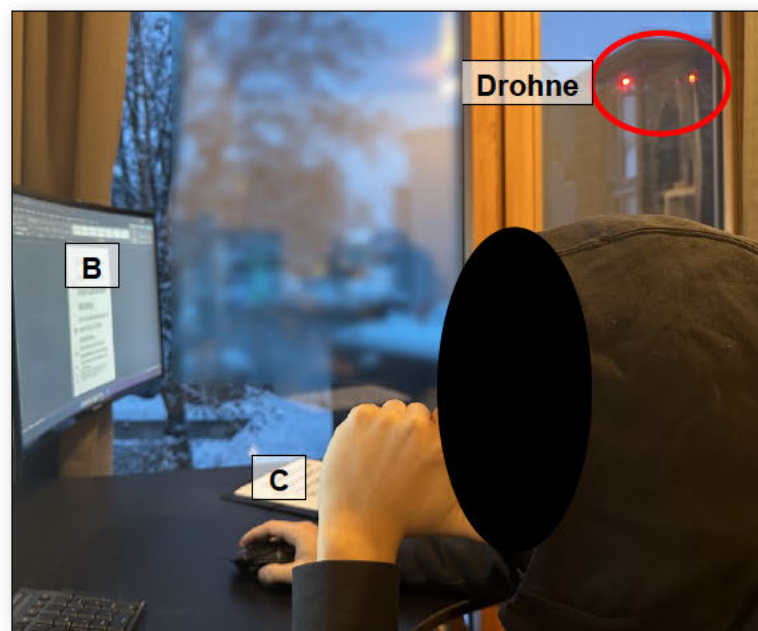


Abbildung 15: Teilnehmer während des Versuchs

Auf den Flugpfaden P1 und P2 befindet sich die Drohne jedoch außerhalb des Sichtfeldes der Teilnehmer. Die obenstehende Abbildung 15 zeigt exemplarisch einen Teilnehmer während des Versuchs. Die Drohne befindet sich hierbei auf dem Flugpfad P2.

Mit dieser niedrigen Entdeckungswahrscheinlichkeit, sowie den Ergebnissen aus der vorherigen Kernfrage lässt sich ein hohes Gefahrenpotenzial des untersuchten Szenarios ableiten. Die folgende und letzte Kernfrage soll nun eine mögliche Abwehrmaßnahme untersuchen, welche das untersuchte Szenario verhindern soll.

6.2.4 Kernfrage Abwehr

Während der Durchführung der Interviews im Rahmen des Kapitels 5, identifizierten Experten (I2, I4, I5) den Einsatz von Strahlenschutzfolien an den Fenstern eines Gebäudes als mögliche Abwehrmaßnahmen gegen das untersuchte Szenario. Die Effektivität dieser Abwehrmaßnahme soll jetzt mit der Beantwortung der Kernfrage um die Abwehr untersucht werden. Im Rahmen des Versuchs wird zur Abschirmung der Fenster eine Rettungsdecke eingesetzt. Sie bietet visuell ähnliche Charakteristiken wie herkömmliche Sichtschutzfolien. Im Vergleich zu den von einigen Experten beschriebenen metallbedampften Scheiben hat sie eine deutlich höhere visuelle Abschirmung. Die Lichtdurchlässigkeit auf beiden Seiten der Folie ist auf der folgenden Abbildung 16 jeweils aus Innen- und Außenansicht dargestellt.



Abbildung 16: Versuchsaufbau Abwehr außen (links) und innen (rechts)

Im Rahmen der Beantwortung dieser Kernfrage wird nun der eingangs beschriebene Versuchsaufbau erneut untersucht. Hierbei wird erneut versucht, sensible Informationen mithilfe der Kamera der Drohne auszulesen. Im ersten Schritt wird ein Kontrollversuch ohne Folie durchgeführt. Anschließend wird die Folie an das Fenster F angebracht. Nun versuchen die Durchführenden, die sensiblen Informationen erneut auszulesen. Der Versuch wird sowohl zur Tages- als auch zur Nachtzeit wiederholt. Hintergrund dafür ist das verschiedene Verhalten von Sichtschutzfolien bei veränderten Lichtverhältnissen. So ist die Sichtschutzfolie immer in Richtung dunkler zu heller Umgebung lichtdurchlässig. Diese Gegebenheiten ändern sich bei schlechten Lichtverhältnissen, da die Lichtquelle im Raum heller ist als das verbleibende Restlicht außerhalb des Fensters.

Bei den Versuchen zur Tageslichtzeit lässt sich erfolgreich die Effektivität der Abwehrmaßnahme feststellen. So lässt die angebrachte Sichtschutzfolie keine Rückschlüsse auf Bildschirminhalte zu. Die folgende Abbildung 17 zeigt die Ansicht der Drohne mit und ohne angebrachte Sichtschutzfolie auf dem Flugpfad P 1. Während ohne die angebrachte Folie die Inhalte des ausliegenden Dokumentes bis zu einer Schriftgröße von 28 Punkt eindeutig zu erkennen sind, lassen sich bei angebrachter Folie keinerlei Informationen über die Gegebenheiten im Raum ableiten.



Abbildung 17: Außenansicht mit (rechts) und ohne (links) Sichtschutzfolie

Bei der Durchführung des Versuchs bei Nacht konnte ebenfalls die Wirksamkeit der Sichtschutzfolie festgestellt werden. Jedoch lassen sich von außen Informationen über die Gegebenheiten im Raum ableiten, da die Sichtschutzfolie nun von innen nach außen die Sicht blockiert. Durch die allgemeine Verdunkelung der Folie und die schlechteren Lichtverhältnisse ist es jedoch der Kamera an der Drohne im Rahmen dieses Versuchs nur bedingt gelungen, sensible Informationen auszulesen. Die folgende Abbildung 18 zeigt die erlangten Ergebnisse bei einem Nachtflug mit der Drohne.

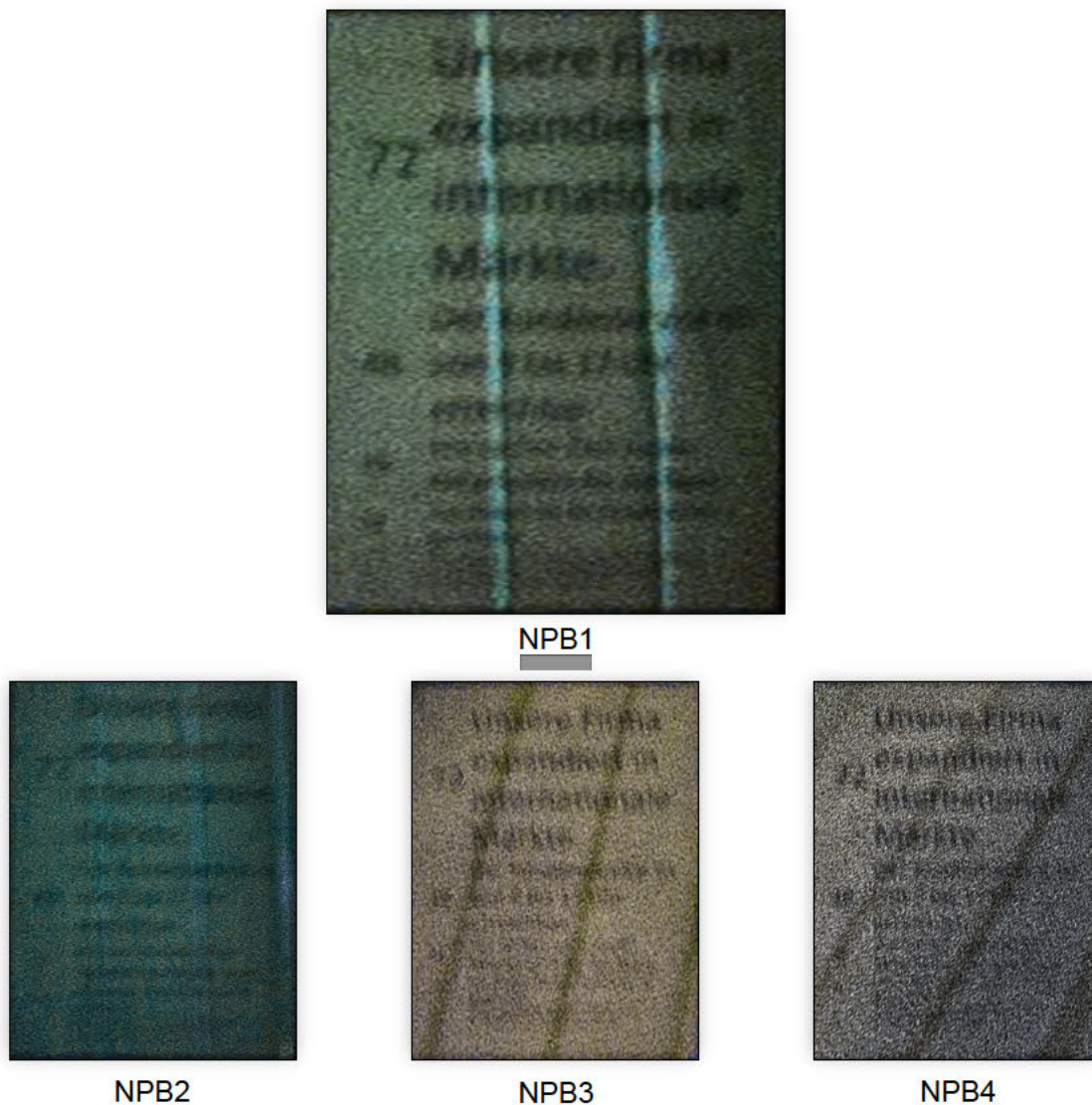


Abbildung 18: Inhalte des Monitors B bei Nacht

Wie zu sehen ist, lassen sich die ungefähren Textinhalte des Bildschirms Schriftgröße 72 ausmachen. Das Auslesen von Texten in kleineren Schriftgrößen ist nicht möglich. Hierbei ist zu beachten, dass lediglich die Inhalte des Monitors und nicht des Dokumentes ausgelesen werden konnten, da dieser über eine Hintergrundbeleuchtung verfügt. Dies gilt, sowohl wenn der Raum beleuchtet ist, als auch wenn die Beleuchtung im Raum ausgeschaltet ist. Das Auslesen der Monitorinhalte ist in beiden Fällen möglich, so wurden die Ergebnisse NPB 2 - 4 bei eingeschalteter Raumbeleuchtung erzielt, Ergebnis NPB 1 hingegen bei ausgeschalteter Raumbeleuchtung.

Obwohl es den Durchführenden während des Versuchs möglich war, Daten auszulesen, lässt sich die Effektivität der Sichtschutzfolie jedoch zweifelsfrei feststellen. Bei Nacht ist diese Effektivität eingeschränkt. So ist es Angreifern nachts bedingt möglich Daten auszulesen. Außerdem besteht ein niedrigeres Entdeckungsrisiko der Drohne,

da Personen im Inneren des Gebäudes die Drohne außerhalb, bei abgeklebten Lichtern an der Drohne, nur schwer erkennen können. Die Wahrscheinlichkeit, dass Daten auch bei Nacht auf hintergrundbeleuchteten Monitoren in der Nähe von Fenstern sichtbar sind, ist jedoch deutlich geringer, da die damit Arbeitenden in der Regel ihre Rechner nach Betriebsschluss herunterfahren oder sperren.

Die Durchführung des Experiments hat gezeigt, dass das untersuchte Szenario auch in der Realität eine Gefahr für die Informationssicherheit darstellt. So ist der untersuchte Angriff nicht nur technisch möglich, sondern bietet auch ein geringes Entdeckungsrisiko der angreifenden Drohne. Des Weiteren wurde gezeigt, dass der untersuchte Angriff durch den Einsatz einer Sichtschutzfolie erfolgreich abgewehrt werden kann. Um den Fokus nun zu erweitern und Drohnengefahren allgemein zu betrachten, sollen im folgenden Kapitel verschiedene Abwehrmöglichkeiten identifiziert und evaluiert werden.

7 Abwehrmaßnahmen

Nachdem in den vorangegangenen Kapiteln aktuelle Bedrohungen dargestellt wurden, soll dieser Teil der Arbeit einen Querschnitt der Abwehrmöglichkeiten geben. Dies soll das Bild der aktuellen Lage vervollständigen. Zudem sollen die aktuellen Herausforderungen in diesem Gebiet kurz erläutert werden. Hierzu wird zu Beginn eine Übersicht über den Bereich der Abwehrmaßnahmen von Drohnen gegeben. Diese Betrachtung findet auf einer abstrakten Ebene auf Basis wissenschaftlicher Literatur statt und soll hauptsächlich verschiedene Strategien darlegen. Dies soll die Übertragbarkeit der Erkenntnisse sicherstellen und der Schnelllebigkeit der kommerziellen Systeme in diesem Bereich entgegenwirken. Die Analyse einzelner kommerzieller Systeme ist nicht direkt Teil dieser Arbeit.

7.1 Übersicht

Zu Beginn unterscheidet Forschung [63–66] im Bereich der Drohnenabwehr grundlegend zwei Bereiche. Den ersten Bereich bildet die Erkennung oder Detektion von Drohnen. Diese Art von System nutzt eine oder mehrerer technischer Maßnahmen, um die Präsenz von Flugobjekten festzustellen. Die Präzision der Lokalisierung von Drohnen variiert hierbei. Umgebung, Detektionstechnologie(en), Beschaffenheit und Geschwindigkeit der Flugobjekte sind hierbei maßgebliche Faktoren [67]. Unter optimalen Bedingungen sind Detektionssysteme in der Lage, die Position von Drohnen dreidimensional zu bestimmen und zu verfolgen. Die Bestimmung des Drohnenmodells sowie der Zuladung ist in bestimmten Fällen ebenfalls möglich. Um die Bestimmung dieser Eigenschaften zu ermöglichen, müssen Erkennungssysteme verschiedene Technologien einsetzen. Alle haben jeweils Vor- und Nachteile. Die wesentlichen Technologien, die in diesem Kontext eingesetzt werden, sind in der folgenden Tabelle 5: Technologien zur Drohnenerkennung aufgeführt.

Methode	Reichweite	Möglichkeiten	Negative Einflussfaktoren
Akustik	~200 m	Detektion, Identifikation, Lokalisierung, Zuladungserkennung	Hintergrundgeräusche
Funk	~1 km	Detektion, Identifikation, Lokalisierung	Wetter, Interferenz, autonome Drohnen
Radar	~100 km	Detektion, Identifikation, Lokalisierung, Verfolgung	Kleine Drohnen, Verwechslungen mit Vögeln oder anderen Objekten
Visuell	~100 m	Detektion, Identifikation, Verfolgung, Zuladungserkennung	Schlechte Sichtverhältnisse

Tabelle 5: Technologien zur Drohnenerkennung aus [67]

Viele Systeme setzen eine Kombination dieser Technologien ein, um bessere Ergebnisse bei der Detektion zu erzielen. Hierbei sollen die Stärken jeder Technologie abhängig von den aktuellen Gegebenheiten optimal genutzt werden.

Alle untersuchten Detektionssysteme teilen die Eigenschaft, dass sie den Flug von unbefugten Drohnen lediglich „beobachten“ können. Sie können keine Maßnahmen ergreifen, um den weiteren Betrieb dieser zu verhindern. Diese Möglichkeit bietet die zweite Kategorie von Systemen zur Drohnenabwehr. So bedienen sich Mitigations- oder Abwehrsysteme einer Reihe von Möglichkeiten, um den weiteren Flug von Drohnen zu unterbrechen. Die verschiedenen Möglichkeiten sind in der folgenden Abbildung 19 aufgeführt. Wie bei den Detektionssystemen auch, bietet jeder Ansatz eigene Vor- und Nachteile. Um die Effizienz der Abwehr zu erhöhen, werden diese Maßnahmen oft zusammen mit einem Detektionssystem eingesetzt.

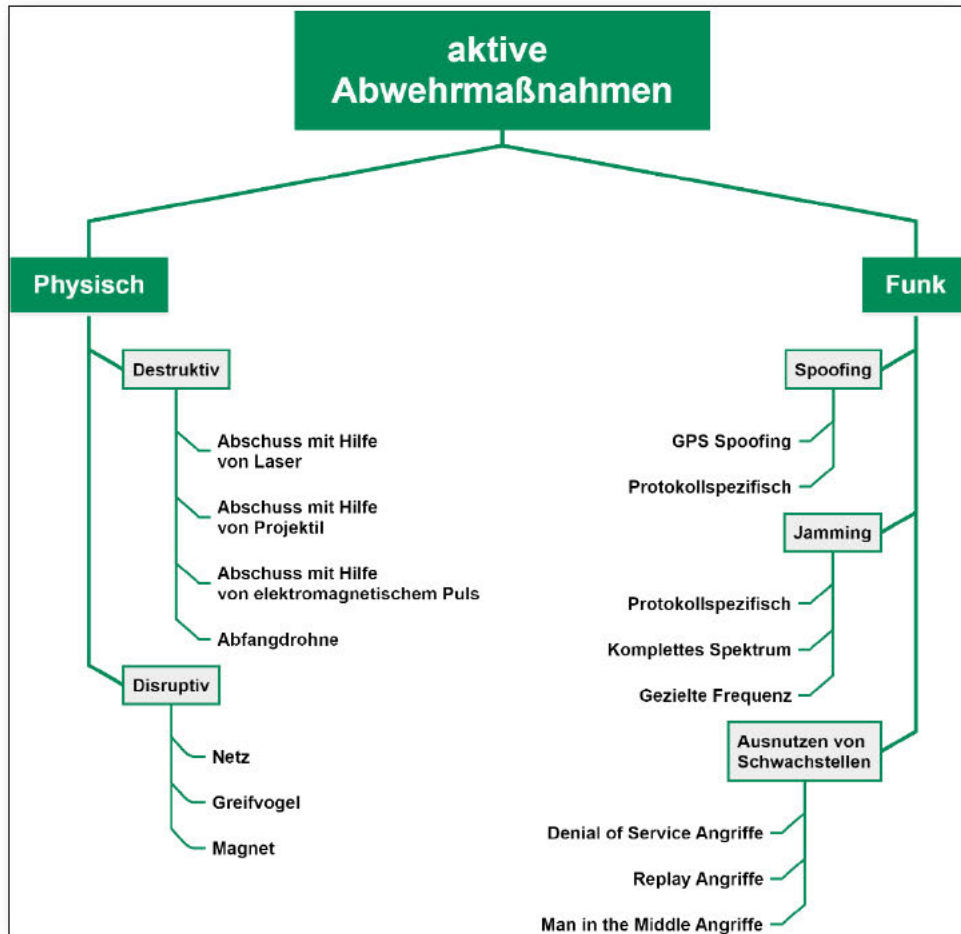


Abbildung 19: Übersicht aktive Abwehrmaßnahmen aus [63, 66]

Die genaue Funktionsweise der einzelnen Strategien werden im Rahmen dieser Arbeit nicht vollumfänglich erläutert. Grundsätzlich verfolgt jeder dieser Ansätze das Ziel, eine Drohne zu Boden zu bringen. Die Landung der Drohne ist hierbei, je nach Ansatz, entweder kontrolliert, unkontrolliert oder teilkontrolliert. Die destruktiven Ansätze führen hierbei oft den unkontrollierten Absturz hervor. Einige disruptive sowie Spoofingansätze dahingegen ermöglichen oft das kontrollierte Landen der abzuwehrenden Drohne, da entweder die Steuerung der Drohne übernommen oder diese in der Luft physikalisch festgesetzt wurde. Die teilkontrollierte Landung wird bei Jamming oder Denial of Service Angriffen herbeigeführt. Hierbei sinkt die Drohne entweder langsam zu Boden oder fliegt, je nach technischer Ausstattung der Drohne, zum Startpunkt zurück.

Eine weitere Art der Abwehrmaßnahmen, welche besonders im Kontext der untersuchten Forschungsfrage relevant ist, wurde während der Experteninterviews, welche im Rahmen dieser Arbeit geführt wurden, identifiziert. So können Organisationen neben technischen Maßnahmen auch bauliche und organisatorische Maßnahmen treffen, um sich gegen einige der identifizierten Drohnen Gefahren zu schützen. In der

folgenden Tabelle 6: Übersicht über Maßnahmen aus den Interviews werden die genannten Maßnahmen aufgeführt. Art bezeichnet hierbei, ob die Maßnahme organisatorisch oder baulich ist. ID bezeichnet den Interviewpartner, welcher die Maßnahme genannt hat.

ID	Art	Maßnahme
I1, I4, I5	Organisatorisch	Schulung der Mitarbeiter zum Erkennen von Drohnen
I1	Organisatorisch	Erstellen eines Notfallkonzepts bei Sichtung einer unbefugten Drohne
I4	Organisatorisch	Regeln zum Verbot von Drohnenflügen auf dem Gelände
I6	Organisatorisch	Clean Desk Policy
I2, I4, I5	Baulich	Abkleben der Fenster mit abschirmender Folie
I4, I5	Baulich	Abschatten der Fenster
I2	Baulich	Besprechungsräume in der Mitte von Gebäuden platzieren
I2	Baulich	Firmengebäude in für Drohnenflug ungünstiges Gelände wie bewaldeten Gebieten bauen

Tabelle 6: Übersicht über Maßnahmen aus den Interviews

Vorteil der meisten dieser Maßnahmen sind die vergleichsweise niedrigen Kosten und die Einfachheit der Umsetzung. So könnten etwa Schulungen für Mitarbeiter im Rahmen anderer Schulungen erfolgen. Notfallkonzepte und Regeln zum Flugverbot müssen einmal erstellt werden und es bedarf im Gegensatz zu technischen Maßnahmen keiner weiteren Betreuung. Welche weiteren Herausforderungen im Bereich der Drohnenabwehr existieren wird nun im Folgenden Unterkapitel weiters untersucht.

7.2 Herausforderungen

Auch wenn die verschiedenen Ansätze teils eine hohe Effizienz bei der Abwehr aufweisen, gibt es eine Reihe von Herausforderungen, welche bei der Drohnenabwehr zu beachten sind. Diese werden in diesem Kapitel betrachtet.

Ein generelles Problem bei der Bekämpfung von Drohnen ist die eindeutige Feststellung der Intention der Drohne. Dieses Problem wird von [68] auch als „Purpose Detection Problem“ bezeichnet. Besonders in urbanen Szenarien und bei Flügen an der Grenze des Firmengeländes zeigt sich die Relevanz des Problems. So könnte eine Drohne, welche nahe dem Firmengelände fliegt, entweder einen legitimen oder einen maliziösen Zweck verfolgen. Die folgende Abbildung 20 illustriert das Problem.

So könnten die Steuernden der Drohne diese zu legitimen Zwecken der Freizeitfotografie nutzen (Bild c). Ändert sich die Ausrichtung der Kamera, so könnte die Drohne auch zum Zweck der Erlangung von sensiblen Informationen verwendet werden (Bild b).

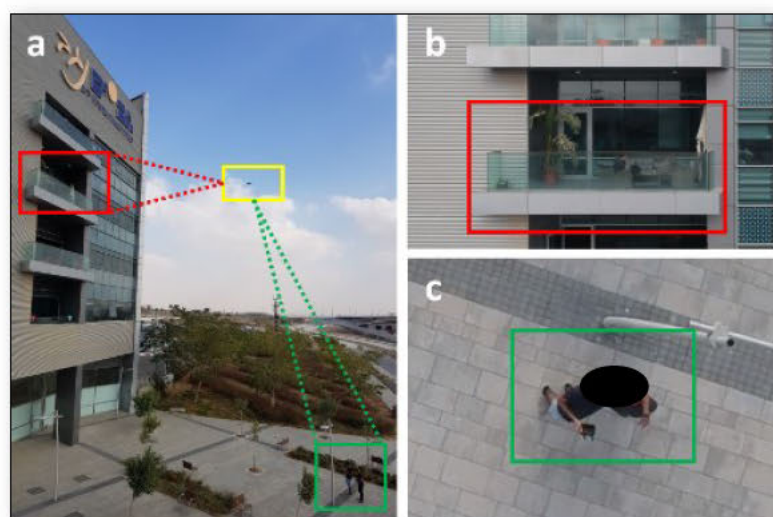


Abbildung 20: Beispiel für das Purpose Detection Problem aus [68]

Dieses Problem lässt sich auch mit Kenntnis über die Kameraausrichtung nicht in jedem Fall lösen, da es Szenarien gibt, in denen das Firmengelände zwangsläufig Teil des Motivs ist. Die Intention liegt daher rein beim Steuernden, welcher sich nicht in unmittelbarer Nähe der Drohne befinden muss.

Neben dieser grundlegenden Herausforderung bringt der Einsatz von technischen Systemen für die Drohnenabwehr eine Reihe weiterer Hürden. Für wirtschaftliche Organisationen spielt hier vorwiegend der monetäre Faktor eine maßgebliche Rolle. Aufgrund der Vielzahl an komplexen technischen Systemen sind die Anschaffungskosten von Detektions- und Abwehrsystemen sehr hoch. So nannte I2 ungefähre Kosten von 300.000 € - 400.000 € für ein nicht weiter beschriebenes Abwehrsystem. Vor allem für kleinere Unternehmen stellt diese Investition eine große finanzielle Herausforderung dar. Die fragliche Wirtschaftlichkeit solcher Systeme bestätigen auch I1, I2, I5 und I6. Doch auch wenn diese Mittel aufgewendet werden können, ist der Einsatz eines Abwehrsystems nicht risikofrei. Im Bereich der Detektionssysteme sind dies zum einen Gegebenheiten der Umgebung und die Einhaltung des Datenschutzes. Beispielsweise können funkbasierte Systeme in stark funkbelasteten Bereichen nicht zuverlässig eingesetzt werden, da Systeme dritter unter Umständen falsche Detektionsergebnisse erzeugen können. Wie I3 anmerkt, können auch Hintergrundgeräusche bei akustischen Systemen zu Fehlern führen. Bei Detektionssystemen, welche

visuelle Detektionsmaßnahmen meist in Form von ständig aktiven Kameras einsetzen, gilt es stets datenschutzrechtliche Rahmenbedingungen einzuhalten.

Weitaus größere Hürden sind auch im Bereich der Abwehrsysteme festzustellen. Sinn der Abwehrsysteme ist es, den weiteren Betrieb von Drohnen zu verhindern. Dieser Prozess involviert immer die selbst induzierte Änderung der Flugroute der Drohne. Mit dieser verursachten Änderung der Flugroute eröffnet sich die Frage der Haftung für entstandene Schäden, da nicht garantiert werden kann, dass die abgefangene Drohne sicher landet. Das Risiko eines Absturzes ist bei der Übernahme der Drohne zwar vergleichsweise gering, werden jedoch destruktive Abwehrmaßnahmen ergriffen, stellt der Absturz den Erfolg der Abwehr dar. Aber nicht nur durch den Absturz einer abzuwehrenden Drohne kann Schaden entstehen, auch beim Einsatz von Jammern, elektromagnetischen Pulsen, GPS, Spoofing oder Lasern zur Abwehr, können ungewollte Interferenzen mit eigenen oder Fremdsystemen auftreten. Je nach Umgebung kann auch hierdurch maßgeblicher Sach- oder Personenschaden entstehen.

All diese Hürden stellen die Abwehr von Drohnen als herausfordernde Disziplin für Organisationen dar. Die Abwägung einer Reihe an wirtschaftlichen und ethischen Faktoren ist notwendig, um über Maßnahmen zur Drohnenabwehr zu entscheiden.

8 Diskussion

Ziel dieser Arbeit war es, die aktuelle Gefährdungslage von frei erhältlichen Drohnen auf die Informationssicherheit von Organisationen zu untersuchen. Im folgenden Kapitel sollen die Ergebnisse nun zusammengeführt und differenziert werden. Zur Beantwortung der Forschungsfrage wurden vier Ansätze verfolgt. Zu Beginn wurde eine Literaturanalyse durchgeführt, welche mögliche Gefahren identifizieren sollten. Des Weiteren wurden sechs Experteninterviews geführt, um die aktuelle Lage sowie weitere mögliche Gefahren von Drohnen auf die Informationssicherheit zu erfassen. Der nächste Ansatz umfasste eine Fallstudie, in welcher die Machbarkeit, das Entdeckungsrisiko sowie eine Abwehrmaßnahme gegen Drohnen untersucht wurden. Im letzten Ansatz wurden dann einige Möglichkeiten zu Drohnenabwehr aufgezählt sowie deren Risiken erläutert. Dies soll exemplarisch eine prägnante Zusammenfassung der aktuellen Lage von Abwehrsystemen darstellen. Die Kombination aus den Erkenntnissen aller vier Ansätze zeigte allgemein, dass Drohnen eine Gefahr für die Informationssicherheit darstellen können. Anhand dieser Forschung erlangt diese Arbeit fünf Kernerkenntnisse. Diese werden im Folgenden erläutert und deren Implikationen interpretiert.

8.1 Vielfalt von Drohnenbedrohungen

Vornehmlich die Ergebnisse der Literaturanalyse zeigten, dass die Angriffe mit Drohnen sehr vielfältig sein können. Im Rahmen dessen wurden vornehmlich zwei Methodiken zum Erlangen von Informationen identifiziert.

Zum einen sind speziell Angriffe auf drahtlose Technologien wie WLAN, DECT, Bluetooth oder auch proprietäre Peripherie Protokolle, für einen durch Drohnen unterstützten Angriff, besonders verwundbar. Drohnen können hierzu spezialisierte Funkhardware an schwer erreichbare Orte auf dem Firmengelände verbringen. Von dort aus können eine Vielzahl von Angriffen, wie das Abhören von Informationen, das Senden falscher Informationen oder das Stören der Kommunikation, durchgeführt werden. Durch die hohe Mobilität durch Drohnen sind nicht nur WLAN-Netzwerke, sondern auch Technologien mit kürzerer Reichweite wie Bluetooth oder Industrieprotokolle betroffen. In Anbetracht der zunehmenden Vernetzung in der Industrie [69] kann dies besonders für produzierende Unternehmen existenzbedrohende Auswirkungen haben.

Zum anderen ist der Einsatz der oft mitgelieferten, hochauflösenden Kameras an Drohnen ein Risiko für die Informationssicherheit. Sie eröffnen eine Reihe an Möglichkeiten zum Ausspähen von Informationen. Auch hierbei zeigt sich wieder die

Vielfältigkeit beim Einsatz von Drohnen. So beschränken sich die technischen Möglichkeiten von Drohnen nicht rein auf den Einsatz kleiner, leistungsschwacher Kameras. Mit Hilfe spezieller Aufhängungen können auch leistungsstarke professionelle Kameras, Wärmebildkameras oder andere Multispektrale Kameras zum Ausspähen von Informationen genutzt werden.

Im Allgemeinen gilt es zu beachten, dass die Auflistung von Gefahren in dieser Arbeit keineswegs vollständig ist. Ziel war es, exemplarisch aufzuzeigen, welches Potenzial preiswerte Drohnen in den Händen kreativer Angreifer haben können. Die vielfältigen Einsatzmöglichkeiten von Drohnen fasst I1 in folgendem Zitat prägnant zusammen: *„[Mit einer] Drohne kannst du 1000 Sachen vorbereiten, von Ausspähen bis zum Abwerfen, bis zum physikalischen Angriff, Kameras an Fenster kleben. [Drohnen sind] halt ein Werkzeug.“* (I1, Pos. 16)

Diese Diversität der Einsatzmöglichkeiten von Drohnen hebt auch die Notwendigkeit für weitere Forschung in dem Bereich hervor. So könnte die Durchführbarkeit mithilfe von Praxisversuchen untersucht werden. Auch eine weitere, tiefgreifende Betrachtung und Aufzählung von möglichen Angriffen könnte die Bedrohungslage umfassender beleuchten.

8.2 Potenzial von Angriffen

Nicht zuletzt durch den Beweis der Machbarkeit eines Angriffs im praktischen Teil dieser Arbeit kann das Potenzial von Angriffen auf die Informationssicherheit mit Drohnen festgestellt werden. Auch die Feststellung einer niedrigen Entdeckungswahrscheinlichkeit von Drohnen in Kombination mit niedrigen Kosten und hoher Verfügbarkeit der Hardware bieten einen attraktiven Angriffsweg für maliziöse Dritte. Ein weiterer Vorteil von Angriffen mithilfe von Drohnen ist auch das gewisse Maß an Anonymität, welches durch die Distanz zwischen der Drohne und dem Steuernden zustande kommt. So können Drohnen je nach Hardware aus Entfernungen von bis zu 35 km [17] gesteuert werden. Erfolgt die Steuerung mit Hilfe von Mobilfunktechnologien, ist diese Entfernung je nach Netzabdeckung praktisch unbegrenzt. Diese Möglichkeit zum Steuern von Drohnen wird auch mit dem Fortschreiten des 5G-Ausbaus in Zukunft [70] an Brisanz gewinnen. Alternativ könnten auch frei erhältliche autonome Systeme genutzt werden, welche automatisiert vordefinierte Missionen ohne das Eingreifen von Piloten abfliegen und so Funkhardware platzieren können.

Betrachtet man zusätzlich noch die in der Gefahren-Tabelle 3 aufgeführten Gefahren, welche technisch eine niedrige Komplexität, geringe Kosten und einen hohen Schaden versprechen, lässt sich eindeutig ein hohes Potenzial von Angriffen mit Drohnen

feststellen. Anhand des hohen Potenzials und der Vielzahl von Faktoren, welche die Durchführung von Drohnenangriffen auf die Informationssicherheit erleichtern, können Vermutungen für die künftige Lage der Bedrohungen angestellt werden. Im Verlauf der Interviews waren sich alle Interviewten sicher, dass es in Zukunft häufiger zu informationssicherheitsbezogenen Zwischenfällen mit Drohnen kommt. Das Ausmaß der steigenden Häufigkeit variierte zwischen den Aussagen der Experten von leichtem Anstieg zu signifikantem Anstieg. Die Interviewpartner finden hierfür verschiedene Erklärungen, drei Interviewpartner nannten den Preisverfall in den Bereichen Drohnen undameratechnik als maßgeblichen Faktor. I3 nannte den allgemeinen Anstieg an Drohnen im Alltag als mögliche Ursache. Durch den prognostizierten Anstieg von Drohnen [71] im Alltag könnte es Angreifern ermöglicht werden, kommerzielle Drohnen zu übernehmen und für eigene Zwecke einzusetzen. Außerdem könnte die allgemeine Gewöhnung der Bevölkerung an Drohnen das Entdeckungsrisiko weiter senken. Eigene Drohnen könnten auch in der Masse der sonstigen Drohnen unentdeckt bleiben. Auch künftig könnte das Potenzial von Angriffen mit Drohnen zu einem Anstieg in Zwischenfällen führen. Firmen könnten so gezwungen werden, sich mit dem Thema der Drohnenabwehr auseinandersetzen zu müssen. Auch hier könnte die Erhebung von aktuellen und historischen Daten über Drohnenzwischenfälle eine akkuratere Voraussage über die Entwicklung der Situation ermöglichen.

8.3 Herausforderungen bei der Abwehr

Im Rahmen der Evaluation der verschiedenen Abwehrmaßnahmen wurde festgestellt, dass es bereits eine Reihe an technischen Möglichkeiten gibt, Drohnen zu detektieren und aktiv abzuwehren. Zum Erreichen dieses Ziels werden in der Regel die Ergebnisse verschiedener Systeme fusioniert, um eine zuverlässige Erkennung sicherzustellen. Bei der Abwägung der verschiedenen Möglichkeiten zur Abwehr stellte sich heraus, dass der Einsatz von aktiven Abwehrsystemen eine Reihe von signifikanten Herausforderungen mit sich bringt. So spielt nicht nur der oft hohe Kostenpunkt von solchen Systemen eine Rolle. Auch das Potenzial von Sach- und Personenschäden ist bei der Abwehr von Drohnen mithilfe aktiver Maßnahmen nicht unbedeutend. Die Betrachtung der verschiedenen Systeme suggeriert, dass es aktuell kein kosteneffizientes System zur Drohnenabwehr oder zur Drohnenerkennung gibt, welches zuverlässig auch für kleine und mittelständische Unternehmen mit vertretbarem Aufwand und unter Einhaltung gesetzlicher Rahmenbedingungen einsetzbar ist. Im Rahmen des praktischen Versuchs wurde jedoch auch gezeigt, dass es nicht immer technischer Systeme bedarf, um Drohnengefahren abzuwehren. So können bereits kosteneffiziente Maßnahmen wie das Anbringen von Sichtschutzfolien oder das

Einführen einer Clean Desk Policy effektiven Schutz gegen Drohnen Gefahren bieten. Die Entscheidung über den Umfang und die genaue Beschaffenheit und Maßnahmen zur Drohnenabwehr ist von jedem Unternehmen unter Betrachtung von Kosten und Nutzen selbst zu treffen. Unter den Experten gab es keinen, dem offizielle Handlungsempfehlungen oder gesetzlichen Richtlinien über Drohnen Gefahren bekannt waren. Mit der zuvor prognostizierten künftigen Relevanz des Themas wäre auch Forschung in diesem Bereich sinnvoll. So könnte die Evaluierung von Abwehrmaßnahmen zum Beispiel im Rahmen einer Vergleichsarbeit tiefgreifender durchgeführt werden. Dadurch könnten konkrete Handlungsmaßnahmen zum Schutz von Unternehmen erstellt werden.

8.4 Eintrittswahrscheinlichkeit von Drohnen Gefahren

Im Rahmen dieser Arbeit wurden eine Vielzahl von Gefahren identifiziert, die Machbarkeit bestätigt und das Entdeckungsrisiko des untersuchten Angriffs als gering eingestuft. Jedoch ist es aufgrund der dünnen Forschungslage im untersuchten Fachbereich sowie fehlenden Berichten aus der Praxis schwer, die allgemeine Eintrittswahrscheinlichkeit der identifizierten Gefahren zu bestimmen. So können Gefahren zwar anhand von Faktoren wie Kosten, Komplexität und Schadenspotenzial ungefähr eingestuft werden, jedoch fehlen historische Daten, um quantitativ fundierte Aussagen, über die Eintrittswahrscheinlichkeit zu treffen. Um trotzdem eine diesbezügliche Indikation zu bekommen, können die Aussagen, welche die Experten während der Interviews tätigten, herangezogen werden. So ordnet I4 die Angriffe auf die Informationssicherheit mithilfe von Drohnen wie folgt ein: *„die Angriffshäufigkeit [...] sollte verschwindend gering sein, wenn man Verstöße gegen den Datenschutz [...] ausschließt. [...] Also diese schon eher theoretischen Szenarien, das sind klare Formen von Targeted Attacks, wo man ganz genau wissen muss, was man tut. Und sehr gut vorbereitet sein und das wird [...] kein massenhafter Angriff, vor allem, weil das ja auch ein erhöhtes Gefahrenpotenzial für den Angreifer bedeutet, weil man sich in unmittelbarer Nähe des Ziels befinden muss, was [...] Cyberkriminelle relativ ungern tun.“* (I4, Pos. 10) Die von I4 genannten Punkte über zwingende Lokalität und Vorwissen bei Angriffen sind valide Punkte, die bei der Einschätzung der Eintrittswahrscheinlichkeit und der Gesamtbetrachtung einbezogen werden sollten. Diese zwei Faktoren schränken die Menge an potenziellen Angreifern deutlich ein und stellt ein deutliches Gegenargument in Bezug auf das Risiko für Angreifer dar.

Auch durch die Aussagen des Interviewpartners I2 lässt sich eine eher geringere Eintrittswahrscheinlichkeit vermuten. So stellt I2 den Mehrwert von Drohnen bei Angriffen auf die Informationssicherheit wie folgt allgemein infrage: *„aus IT Security Perspektive*

bzw. aus IT Diebstahl Sicht sehe ich keine Punkte, [bei denen] die Drohne einen Vorteil hätte gegenüber anderen Mechanismen, die weitaus einfacher [sind].“ (I2, Pos. 21). Eine ähnlich kritische Betrachtung des Mehrwerts von Drohnen vertritt auch I3 im Rahmen des Interviews. Die Interviewpartner nennen hier etwa den Einsatz von Innentätern zur Verbringung von Hardware oder die Interaktion mit Funksignalen, welche über die Grundstücksgrenzen heraus strahlen. Auch wenn für den Rahmen dieser Arbeit keine eindeutigen Fallbeispiele oder Statistiken identifiziert werden konnten, die diese These eindeutig bestätigt oder widerlegt, kann man doch unter Anbetracht der zuvor genannten Vorteile von Angriffen mit Drohnen in die entgegengesetzte Richtung der Aussagen argumentieren. In jedem Fall stellt diese Infragestellung jedoch auch einen Indikator dafür dar, dass Angriffe auf die Informationssicherheit mit Drohnen tendenziell von eher besser organisierten Dritten durchgeführt werden.

Um fundierte Rückschlüsse auf die allgemeine Eintrittswahrscheinlichkeit von Angriffen zu ziehen, liegen zum Zeitpunkt der Arbeit nicht ausreichend Materialien in Form von Forschungsstatistiken oder Praxisberichten vor. Auf Basis der Voraussetzungen der Angriffe sowie der Aussagen der Experten lässt sich jedoch vermuten, dass Angriffe auf die Informationssicherheit mithilfe von Drohnen grundsätzlich von organisierten Dritten durchgeführt werden. Weitere Forschung und Datenerhebung im Bereich der Häufigkeit von Angriffen würden die aktuelle Bedrohungslage in der Realität weiter beleuchten.

Es ist an dieser Stelle erneut zu betonen, dass sich die Forschung im Rahmen dieser Arbeit rein auf den nicht destruktiven Einsatz von Drohnen beschränkt. Die Experten betonten im Verlauf der Interviews wiederholt, dass der Einsatz von Drohnen zu destruktiven oder terroristischen Zwecken ein realistisches Risiko darstellt. Sie beziehen sich hierbei nicht nur auf die Beeinträchtigung des Betriebs durch Zerstörung technischer Anlagen, sondern auch durch die Induzierung von Personenschäden oder die Androhung derselben. Der gefährdende Einsatz von Drohnen sowie die Bewertung der Effektivität von militärischen Abwehrsystemen ist nicht Teil dieser Arbeit.

8.5 Stand der Forschung des Fachgebietes

Die letzte Erkenntnis dieser Arbeit bezieht sich auf den aktuellen Forschungsstand in dem Bereich. Der Einsatz von Drohnen zum allgemeinen Erlangen von Informationen ohne den Einsatz destruktiver Maßnahmen ist aktuell noch ein exploratives Forschungsfeld, welches laut der Experten künftig an Relevanz gewinnt. So wurde festgestellt, dass benachbarte Bereiche bereits bestand aktueller Forschung sind. Einer dieser Bereiche ist die Härtung von Drohnen gegen Cyberangriffe. Die

Forschungsarbeiten hierzu sind vielfältig und reichen von der Untersuchung der Hardwaresicherheit zur Absicherung von Drohnen gegen Angriffe bis hin zur Sicherheit in der Kommunikation zwischen Drohnen und ihren Steuerungssystemen. Ein weiterer Schwerpunkt liegt im destruktiven militärischen Einsatz von Drohnen, der bereits Gegenstand einiger Forschungsarbeiten war. Dieses Feld umfasst Untersuchungen zur Nutzung von Drohnen für terroristische Zwecke sowie zur Terrorismusabwehr. Diese Aspekte der Drohnenforschung sind insofern relevant für diese Arbeit, als dass sie ein Licht auf die potenziellen Bedrohungen und Abwehrmechanismen in Bezug auf Drohnen werfen, die für die Informationssicherheit von Organisationen von Bedeutung sein können. Diese Arbeit ergänzt diese bestehenden Forschungsströmungen, indem sie die spezifischen Bedrohungen von Drohnen für die Informationssicherheit von Organisationen in den Fokus rückt. Während die existierende Forschung sich hauptsächlich auf technische und militärische Aspekte konzentriert, bietet diese Arbeit eine umfassende Analyse der Bedrohungslandschaft im Kontext der Informationssicherheit und untersucht dabei sowohl potenzielle Angriffsszenarien als auch geeignete Gegenmaßnahmen. Dadurch wird die Forschungslücke im Bereich der zivilen Nutzung von Drohnen und deren Auswirkungen auf die Informationssicherheit adressiert. Anhand der Forschungsergebnisse dieser Arbeit lässt sich eindeutig feststellen, dass Drohnen aktuell und künftig ein signifikantes Risiko insbesondere durch die einfache Verfügbarkeit, die niedrige Komplexität und das geringe Entdeckungsrisiko für die Informationssicherheit darstellen können. Bevor weitere Forschung im Bereich der Angriffe oder der Verteidigung gegen Drohnen unternommen wird, ist es sinnvoll, die aktuelle Lage sowie die künftige Entwicklung in diesem Bereich zu untersuchen. So kann proaktiv abgeschätzt werden, in welchem Umfang das Fachgebiet weiter untersucht werden sollte. Die Ergebnisse dieser Arbeit stellen einen Beitrag zur Forschung in dem Bereich dar, da sie einen grundlegenden Überblick über mögliche Gefahren bietet sowie exemplarisch eine diese Gefahren auf Machbarkeit, Entdeckungsrisiko und Verteidigungsmöglichkeiten untersucht. Dadurch konnte die Notwendigkeit künftiger Forschung festgestellt werden.

9 Fazit

Diese Arbeit ging der Frage nach, welchen Gefahren frei erhältliche Drohnen auf die Informationssicherheit von Organisationen darstellen. Um diese Frage zu beantworten und ein aktuelles Bild der Lage diesbezüglich zu bekommen, verfolgte diese Arbeit vier maßgebliche Ansätze. So konnten im ersten Ansatz mithilfe einer Literaturanalyse eine Vielzahl hypothetischer Gefahren aus der Literatur identifiziert werden. Der zweite Teil umfasste das Führen und qualitative Auswerten von Interviews mit Experten, welche weitreichende Einblicke in die aktuelle und künftige Lage von Drohnengefahren und Möglichkeiten zur Drohnenabwehr gaben. Der dritte Ansatz dieser Arbeit umfasste eine praktische Fallstudie, indem mit Hilfe von drei Kernfragen sowohl die Machbarkeit, das Entdeckungsrisiko als auch die Effektivität einer möglichen Abwehrmaßnahme untersucht wurden. Im letzten Teil wurden dann Abwehrmaßnahmen sowie Herausforderungen bei dem Einsatz dieser untersucht. Dieser viersäulige Ansatz deckt das Spektrum von Theorie zu Praxis vollständig ab und ermöglicht die Erstellung eines umfassenden Lagebilds so wie fundierte Vermutungen zu den zukünftigen Entwicklungen in diesem Bereich.

Zu Beginn lässt sich eine deutliche Forschungslücke im nicht destruktiven zivilen Einsatz von Drohnen zur Beeinträchtigung der Informationssicherheit von Organisationen feststellen. Benachbarte Fachgebiete wie die Absicherung von Drohnen selbst oder der destruktive Einsatz von Drohnen so wie die Abwehr im militärischen Bereich sind bereits bestand aktueller Forschung. Der in dieser Arbeit untersuchte jedoch nicht. Des Weiteren stellt die Arbeit fest, dass Drohnen eine Vielzahl von Gefahren für die Informationssicherheit darstellen können. Außerdem zeigte der praktische Versuch anhand eines identifizierten Beispiels, dass Angriffe nicht nur machbar sind, sondern zusätzlich auch ein niedriges Entdeckungsrisiko für Angreifer bieten. Zudem wurde gezeigt, dass der technische Fortschritt im Bereich der Drohnen sowie der Kamertechnik die Machbarkeit und das Ausmaß erlangter Informationen in Zukunft weiter steigern wird. Die Untersuchung verschiedener Methoden zur Drohnenabwehr und Drohnerdetektion zeigen deutliche Herausforderungen in Form von Risiken und Unzuverlässigkeit bei der aktiven Abwehr. Es wurde jedoch auch festgestellt, dass kosteneffiziente bauliche Nachrüstungsmaßnahmen oder organisatorische Schritte effizienten Schutz gegen bestimmte Drohnengefahren bieten können. Neben der potenziellen Gefahr, die von Drohnen ausgeht, wurden auch Indikatoren gefunden, welche die Eintrittswahrscheinlichkeit vieler identifizierten Gefahren als eher gering einstufen,

da oft ein gewisses Maß von Planung und Lokalität für die Durchführung vonnöten ist.

Die möglichen Richtungen weiterer Forschung im untersuchten Bereich sind vielfältig. So könnten im ersten Schritt weitere Untersuchungen über die Eintrittswahrscheinlichkeit oder die aktuelle Häufigkeit von Angriffen auf die Informationssicherheit mithilfe von Drohnen beispielsweise in Form von Umfragen, weiteren Interviews oder Analyse von Zwischenfällen, durchgeführt werden. Wird im Zuge dessen aktuell oder künftig eine maßgebliche Gefahrenlage festgestellt, können die Ergebnisse weiterer Untersuchungen von Angriffsszenarien Einblicke in die Möglichkeiten von Angreifern geben. Außerdem können auch die Abwehrmöglichkeiten weiter untersucht werden. Diese Untersuchungen können auch von den Ergebnissen der Forschung im Bereich der Angreifer profitieren. Durch genaue Untersuchung und Bewertung der Angriffe sowie der Verteidigungsmöglichkeiten können schlussendlich konkrete Handlungsempfehlungen abgeleitet werden, welche unter anderem auch in Rahmenwerke zur Absicherung der Informationssicherheit oder in juristische Schriften gefasst werden können. Diese wissenschaftliche Untersuchung des Fachbereichs trägt besonders unter Beachtung aktueller technologischer Trends im Bereich der Drohnen zur allgemeinen Verbesserung der Sicherheit bei.

Die aktuelle und künftige Relevanz des in dieser Arbeit untersuchten Themas wird auch durch die Annahme dieser Arbeit beim 20. Deutschen IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik unterstrichen.

Literaturverzeichnis

- [1] Statista, *Drone average price worldwide 2018 to 2028 (in 1,000 U.S. dollars)*. [Graph]. [Online]. Available: <https://www.statista.com/forecasts/1399086/drone-average-price-worldwide> (accessed: Dec. 5 2023).
- [2] M. G. Moehrle and H. Caferoglu, "Technological speciation as a source for emerging technologies. Using semantic patent analysis for the case of camera technology," *Technological Forecasting and Social Change*, vol. 146, pp. 776–784, 2019, doi: 10.1016/j.techfore.2018.07.049.
- [3] M. Reger, J. Bauerdick, and H. Bernhardt, "Drohnen in der Landwirtschaft: Aktuelle und zukünftige Rechtslage in Deutschland, der EU, den USA und Japan," (in de), *Landtechnik*, vol. 73, no. 3, 2018, doi: 10.1515/lt.2018.3183.
- [4] BIS Research, *Global sky-based communication market revenue 2031*. [Online]. Available: <https://www.statista.com/statistics/1289151/sky-based-communication-market-revenue-by-application-worldwide/> (accessed: Dec. 5 2023).
- [5] DJI Official, *DJI Mavic 3 Pro – Technische Daten – DJI*. [Online]. Available: <https://www.dji.com/de/mavic-3-pro/specs> (accessed: Dec. 2 2023).
- [6] Statista, *Global: drone market revenue by country 2022*. [Online]. Available: <https://www.statista.com/forecasts/1302524/revenue-of-the-drone-market-worldwide> (accessed: Dec. 5 2023).
- [7] Luftfahrt-Bundesamt (LBA), *Statistiken Unbemannte Luftfahrtsysteme ab 2021*. [Online]. Available: <https://www.lba.de/SharedDocs/Downloads/DE/SBI/SBI3/Statistiken/Betrieb/UAS.html> (accessed: Sep. 29 2023).
- [8] D. Kunertova, "The war in Ukraine shows the game-changing effect of drones depends on the game," *Bulletin of the Atomic Scientists*, vol. 79, no. 2, pp. 95–102, 2023, doi: 10.1080/00963402.2023.2178180.
- [9] D. Kunertova, "The Ukraine Drone Effect on European Militaries," 2022.
- [10] Mark Saunders, Philip Lewis, Adrian Thornhill, M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students, 9th Edition*. Harlow, England, New York: Pearson, 2023.
- [11] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Progress in Aerospace Sciences*, vol. 91, pp. 99–131, 2017, doi: 10.1016/j.paerosci.2017.04.003.
- [12] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends," *Intel Serv Robotics*, vol. 16, no. 1, pp. 109–137, 2023, doi: 10.1007/s11370-022-00452-4.

- [13] Enrique Moya, *EMT-Luna-X-2000-04-20-2019.jpg: (JPEG-Grafik, 950 × 633 Pixel)*. [Online]. Available: <https://www.strategypage.com/gallery/images/EMT-Luna-X-2000-04-20-2019.jpg> (accessed: Dec. 10 2023).
- [14] DJI, *Image of the DJI AGRAS T30*. [Online]. Available: <https://dji-official-fe.djicdn.com/dps/a2d9b21e4f870c162ff4cd6d83a76265.jpg> (accessed: Dec. 10 2023).
- [15] DJI, *DJI Mavic 3 Pro*. [Online]. Available: <https://dji-official-fe.djicdn.com/cms/uploads/9c3ba6cc54de0d24a7fdf07178bae64f.png> (accessed: Dec. 10 2023).
- [16] DJI, *DJI Inspire 3*. [Online]. Available: <https://store.dji.com/de/product/dji-inspire-3> (accessed: Dec. 10 2023).
- [17] ExpressLRS, *Long Range Competition - ExpressLRS*. [Online]. Available: <https://www.expresslrs.org/info/long-range/> (accessed: Sep. 13 2023).
- [18] I. Bor-Yaliniz, M. Salem, G. Senerath, and H. Yanikomeroğlu, "Is 5G Ready for Drones: A Look into Contemporary and Prospective Wireless Networks from a Standardization Perspective," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 18–27, 2019, doi: 10.1109/MWC.2018.1800229.
- [19] EASA, *What is the difference between autonomous and automatic drone? | EASA*. [Online]. Available: <https://www.easa.europa.eu/en/faq/116449> (accessed: Sep. 18 2023).
- [20] J. Glossner, S. Murphy, and D. Iancu, "An Overview of the Drone Open-Source Ecosystem," Oct. 2021. [Online]. Available: <https://arxiv.org/pdf/2110.02260.pdf>
- [21] ArduPilot Dev Team, *ArduPilot Mission Planner*. [Online]. Available: https://ardupilot.org/planner/_images/mission_planner_screen_flight_plan.jpg (accessed: Sep. 18 2023).
- [22] *Yuneec E30Z Optical Zoom Camera Raw Test Footage - 1.2 Mile Line of Sight! - YouTube*. [Online]. Available: https://www.youtube.com/watch?v=I19E7tsZ2_U (accessed: Oct. 3 2023).
- [23] I. Hanschke, *Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten: Eine kompakte Einführung in die Praxis*, 2nd ed. Wiesbaden, Heidelberg: Springer Vieweg, 2020.
- [24] *ISO/IEC 27000:2018: Information technology - Security techniques - Information security management systems - Overview and vocabulary*, ISO/IEC 27000:2018, International Organization for Standardization, Online, Feb. 2018. [Online]. Available: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
- [25] E. von Faber, *IT und IT-Sicherheit in Begriffen und Zusammenhängen: Thematisch Sortiertes Lexikon Mit Alphabetischem Register Zum Nachschlagen*.

- Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2021. [Online]. Available: <https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6511632>
- [26] S. C. Sethuraman, V. Vijayakumar, and S. Walczak, "Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles," *J Med Syst*, vol. 44, no. 1, p. 29, 2019, doi: 10.1007/s10916-019-1489-9.
- [27] S. Voitenko, V. Druzhyinin, H. Martyniuk, and T. Meleshko, "Unmanned Aerial Vehicles as a Source of Information Security Threats of Wireless Network," *IJC*, pp. 377–382, 2022, doi: 10.47839/ijc.21.3.2695.
- [28] C. J. Swinney and J. C. Woods, "A Review of Security Incidents and Defence Techniques Relating to the Malicious Use of Small Unmanned Aerial Systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 37, no. 5, pp. 14–28, 2022, doi: 10.1109/MAES.2022.3151308.
- [29] C. Bunse and S. Plotz, "Security Analysis of Drone Communication Protocols," in *Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, June 26-27, 2018, Proceedings*, 2018, pp. 96–107. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-94496-8_7
- [30] J. Mead, C. Bobda, and T. J. L. Whitaker, "Defeating drone jamming with hardware sandboxing," in *Proceedings of the 2016 IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2016): 19-20 Dec., 2016, Yilan, Taiwan*, Yilan, Taiwan, 2016, pp. 1–6.
- [31] G. Karmakar, M. Petty, H. Ahmed, R. Das, and J. Kamruzzaman, "Security of Internet of Things Devices: Ethical Hacking a Drone and its Mitigation Strategies," in *Proceedings of the IEEE CSDE, December 18-22, 2022, Gold Coast, Australia*, Gold Coast, Australia, 2022, pp. 1–5.
- [32] M. Krichen, W. Y. H. Adoni, A. Mihoub, M. Y. Alzahrani, and T. Nahhal, "Security Challenges for Drone Communications: Possible Threats, Attacks and Countermeasures," in *2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, 2022.
- [33] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones," *Drones*, vol. 7, no. 7, p. 430, 2023, doi: 10.3390/drones7070430.
- [34] A. Jackman, "Consumer drone evolutions: trends, spaces, temporalities, threats," *Defense & Security Analysis*, vol. 35, no. 4, pp. 362–383, 2019, doi: 10.1080/14751798.2019.1675934.
- [35] Z. Kallenborn, G. Ackerman, and P. C. Bleek, "A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism," *Terrorism and*

- Political Violence*, vol. 35, no. 7, pp. 1556–1585, 2023, doi: 10.1080/09546553.2022.2061960.
- [36] R. Heidger, V. Lambercy, and D. Lambers, "Tracking Analysis of Drone Detection Systems at Airports: Methodology and Results," in *2021 21st International Radar Symposium (IRS): 21-22 June 2021*, Berlin, Germany, 2021, pp. 1–17.
- [37] B. Taha and A. Shoufan, "Machine Learning-Based Drone Detection and Classification: State-of-the-Art in Research," *IEEE Access*, vol. 7, pp. 138669–138682, 2019, doi: 10.1109/access.2019.2942944.
- [38] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, "Survey on Anti-Drone Systems: Components, Designs, and Challenges," *IEEE Access*, vol. 9, pp. 42635–42659, 2021, doi: 10.1109/ACCESS.2021.3065926.
- [39] Q. Yue, Z. Li, C. Gao, W. Yu, X. Fu, and W. Zhao, "The Peeping Eye in the Sky," in *2018 IEEE Global Communications Conference (GLOBECOM): Proceedings : Abu Dhabi, UAE, 9-13 December 2018*, Abu Dhabi, United Arab Emirates, 2018, pp. 1–7.
- [40] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao, "My Google Glass Sees Your Passwords!," in *Black Hat USA 2014*. Accessed: Sep. 22 2023. [Online]. Available: <https://www.blackhat.com/docs/us-14/materials/us-14-Fu-My-Google-Glass-Sees-Your-Passwords-WP.pdf>
- [41] Y. Abdrabou, Y. Abdelrahman, A. Ayman, A. Elmougy, and M. Khamis, "Are Thermal Attacks Ubiquitous?," in *Proceedings of the International Conference on Advanced Visual Interfaces*, Salerno Italy, 2020, pp. 1–5.
- [42] N. Alotaibi, J. Williamson, and M. Khamis, "ThermoSecure: Investigating the Effectiveness of AI-Driven Thermal Attacks on Commonly Used Computer Keyboards," *ACM Trans. Priv. Secur.*, vol. 26, no. 2, pp. 1–24, 2023, doi: 10.1145/3563693.
- [43] S. A. Macdonald, N. M. T. Alotaibi, M. S. Islam, and M. Khamis, "Conducting and Mitigating Portable Thermal Imaging Attacks on User Authentication using AI-driven Methods," in *Proceedings of the Augmented Humans International Conference 2023*, Glasgow United Kingdom, 2023, pp. 357–359.
- [44] Y. Qu, T. Wang, and Z. Zhu, "Vision-Aided Laser Doppler Vibrometry for Remote Automatic Voice Detection," *IEEE/ASME Trans. Mechatron.*, vol. 16, no. 6, pp. 1110–1119, 2011, doi: 10.1109/TMECH.2010.2077678.
- [45] J. M. Moses and K. P. Trout, "A Simple Laser Microphone for Classroom Demonstration," *The Physics Teacher*, vol. 44, no. 9, pp. 600–603, 2006, doi: 10.1119/1.2396779.

- [46] H. Zhang, T. Lv, and C. Yan, "The novel role of arctangent phase algorithm and voice enhancement techniques in laser hearing," *Applied Acoustics*, vol. 126, pp. 136–142, 2017, doi: 10.1016/j.apacoust.2017.05.024.
- [47] H. Chen, W. Li, Z. Cheng, X. Liang, and Q. Zhang, "TCS-LipNet: Temporal & Channel & Spatial Attention-Based Lip Reading Network," in 2023, pp. 413–424. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-44201-8_34
- [48] Mark Vink, *A comprehensive taxonomy of wi-fi attacks*. Online, 2020. [Online]. Available: https://www.ru.nl/publish/pages/769526/mark_vink.pdf
- [49] M. Kammerstetter, M. Muellner, D. Burian, C. Kudera, and W. Kastner, "Efficient High-Speed WPA2 Brute Force Attacks Using Scalable Low-Cost FPGA Clustering," in 2016, pp. 559–577. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-662-53140-2_27
- [50] A. Lonzetta, P. Cope, J. Campbell, B. Mohd, and T. Hayajneh, "Security Vulnerabilities in Bluetooth Technology as Used in IoT," *JSAN*, vol. 7, no. 3, p. 28, 2018, doi: 10.3390/jsan7030028.
- [51] S. Khanji, F. Iqbal, and P. Hung, "ZigBee Security Vulnerabilities: Exploration and Evaluating," in *2019 10th International Conference on Information and Communication Systems (ICICS): 11-13 June 2019, Jordan University of Science and Technology, Irbid, Jordan*, Irbid, Jordan, 2019, pp. 52–57.
- [52] I. Sanchez, G. Baldini, D. Shaw, and R. Giuliani, "Experimental passive eavesdropping of Digital Enhanced Cordless Telecommunication voice communications through low-cost software-defined radios," *Security Comm Networks*, vol. 8, no. 3, pp. 403–417, 2015, doi: 10.1002/sec.989.
- [53] *MouseJack, KeySniffer and Beyond: Keystroke Sniffing and Injection Vulnerabilities in 2.4 GHz Wireless Mice and Keyboards*, 2016. [Online]. Available: <https://media.defcon.org/def%20con%2024/def%20con%2024%20presentations/def%20con%2024%20-%20marc-newlin-mousejack-injecting-keystrokes-into-wireless-mice-wp-updated.pdf>
- [54] P. Mayring, *Qualitative Inhaltsanalyse: Grundlagen und Techniken*, 12th ed. Weinheim: Beltz, 2015. [Online]. Available: <http://nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-1136370>
- [55] Bundesamt für Sicherheit in der Informationstechnik, *3.3.2 Schadenskategorien und -szenarien festlegen*. [Online]. Available: <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs->

- Notfallmanagement/3_BusinessImpactAnalysieren/2_SchaedenAnalysieren/1_Kategorien/kategorien_node.html (accessed: Sep. 20 2023).
- [56] Amazon.com Inc., *F450 Drohnen-Bausatz, Rahmen + Pixhawk + GPS + Leistungsmodul + ESC + Bürstenloser Motor + Propeller + Akku + RC-Sender und -Empfänger + Zubehör + Zunftbuch & Video*. [Online]. Available: <https://www.amazon.de/Drohnen-Bausatz-Quadcopter-Kostenloses-Anleitungsbuch-Empf%C3%A4nger/dp/B09SZ7LNXB/> (accessed: Oct. 6 2023).
- [57] J. Zhang and H. Qu, "Improvement of super resolution reconstruction method for real text images," in *2022 International Conference on Machine Learning and Intelligent Systems Engineering: MLISE 2022 : 5-7 August 2022, Guangzhou, China : proceedings*, Guangzhou, China, 2022, pp. 379–382.
- [58] H. Cho, J. Wang, and S. Lee, "Text Image Deblurring Using Text-Specific Properties," in *Computer vision - ECCV 2012: 12th European Conference on Computer Vision, Florence, Italy, October 7 - 13, 2012; proceedings*, 2012, pp. 524–537. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-33715-4_38
- [59] DJI Official, *Mavic Pro - Produktinformationen - DJI*. [Online]. Available: <https://www.dji.com/de/mavic/info> (accessed: Dec. 2 2023).
- [60] DJI Official, *DJI Mini 2 - Technische Daten - DJI*. [Online]. Available: <https://www.dji.com/de/mini-2/specs> (accessed: Dec. 2 2023).
- [61] DJI Official, *DJI Mavic 3 Classic - Technische Daten - DJI*. [Online]. Available: <https://www.dji.com/de/mavic-3-classic/specs> (accessed: Dec. 2 2023).
- [62] YouTube, *DJI MAVIC PRO - HOW MUCH CAN IT LIFT? MAVIC vs PHANTOM COMPARISON*. [Online]. Available: <https://www.youtube.com/watch?v=v3tV55oYEFk> (accessed: Dec. 2 2023).
- [63] J. Wang, Y. Liu, and H. Song, "Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 4–29, 2021, doi: 10.1109/MAES.2020.3015537.
- [64] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi, and J. Chen, "Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 68–74, 2018, doi: 10.1109/MCOM.2018.1700430.
- [65] H. Kang, J. Joung, J. Kim, J. Kang, and Y. S. Cho, "Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems," *IEEE Access*, vol. 8, pp. 168671–168710, 2020, doi: 10.1109/ACCESS.2020.3023473.
- [66] F.-L. Chipper, A. Martian, C. Vladeanu, I. Marghescu, R. Craciunescu, and O. Fratu, "Drone Detection and Defense Systems: Survey and a Software-Defined

- Radio-Based Solution," *Sensors (Basel, Switzerland)*, vol. 22, no. 4, 2022, doi: 10.3390/s22041453.
- [67] M. A. Khan, H. Menouar, A. Eldeeb, A. Abu-Dayya, and F. D. Salim, "On the Detection of Unauthorized Drones—Techniques and Future Perspectives: A Review," *IEEE Sensors J.*, vol. 22, no. 12, pp. 11439–11455, 2022, doi: 10.1109/JSEN.2022.3171293.
- [68] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "SoK: Security and Privacy in the Age of Commercial Drones," in *2021 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May. 2021 - May. 2021, pp. 1434–1451.
- [69] IDATE DigiWorld and ETNO, *Industry IoT active connections EU 2016-2025*. [Online]. Available: <https://www.statista.com/statistics/691870/industry-iot-active-connections-in-the-eu/> (accessed: Dec. 7 2023).
- [70] GSMA and GSMA Intelligence, *Mobile technology share by generation 2016-2030*. [Online]. Available: <https://www.statista.com/statistics/740442/worldwide-share-of-mobile-telecommunication-technology/> (accessed: Dec. 7 2023).
- [71] Roland Berger, *Global cargo drone market size forecast 2022-2030*. [Online]. Available: <https://www.statista.com/statistics/1415129/worldwide-cargo-drone-market-revenue-forecast/> (accessed: Dec. 7 2023).

Abbildungsverzeichnis

Abbildung 1: Übersicht der methodischen Ansätze	4
Abbildung 2: Darstellung der Struktur dieser Arbeit.....	5
Abbildung 3: Verschiedene Bauformen von Drohnen aus [12]	7
Abbildung 4: Beispiele der verschiedenen Drohnenkategorien aus [13–15].....	8
Abbildung 5: Ardupilot Mission Planner aus [21]	10
Abbildung 6: 36x Zoom der E30ZX (ca. 2 km Distanz) aus [22]	12
Abbildung 7: Klassifizierte Bedrohungen.....	32
Abbildung 8: Ampelsystem Gefahrentabelle	33
Abbildung 9: Versuchsaufbau Innenansicht	37
Abbildung 10: Versuch Außenansicht und Flugpfade.....	38
Abbildung 11: Während des Versuchs eingesetzte Drohnen	39
Abbildung 12: Verbesserte Ergebnisse des Dokuments.....	39
Abbildung 13: Verbesserte Ergebnisse des Monitors	40
Abbildung 14: Vergleichsaufnahme mit höherer Auflösung	41
Abbildung 15: Teilnehmer während des Versuchs	43
Abbildung 16: Versuchsaufbau Abwehr außen (links) und innen (rechts)	44
Abbildung 17: Außenansicht mit (rechts) und ohne (links) Sichtschutzfolie	45
Abbildung 18: Inhalte des Monitors B bei Nacht.....	46
Abbildung 19: Übersicht aktive Abwehrmaßnahmen aus [63, 66]	51
Abbildung 20: Beispiel für das Purpose Detection Problem aus [68].....	53

Tabellenverzeichnis

Tabelle 1: Preisvergleich verschiedener Kameratechniken	11
Tabelle 2: Übersicht der Interviewpartner sowie deren fachliches Umfeld.....	29
Tabelle 3: Gefahrentabelle aller Gefahren	34
Tabelle 4: Ergebnisse Entdeckungsrisiko	42
Tabelle 5: Technologien zur Drohnenerkennung aus [67]	50
Tabelle 6: Übersicht über Maßnahmen aus den Interviews.....	52

Abkürzungsverzeichnis

LiDAR	Light detection and ranging, Methode zur optischen Abstands- und Geschwindigkeitsmessung
ELRS	ExpressLRS, Funkprotokoll
LTE	Long Term Evolution, Mobilfunkstandard
GPS	Global Positioning System, Bezeichnung für ein globales Navigationssatellitensystem zur Positionsbestimmung
DSLR	digital single lens reflex, Bezeichnung für eine Art von digitalem Kamerasystem
CIA	Akronym wie in 2.2.1 beschrieben
STRIDE	Akronym wie in 2.2.2 beschrieben
WLAN	Wireless Local Area Network, Bezeichnung für lokale Funknetzwerke
Radar	radio detection and ranging, Erkennungs- und Ortungsverfahren
KI	Künstliche Intelligenz
PKW	Personenkraftwagen
DECT	Digital Enhanced Cordless Telecommunications, Standard für Drahtlose Telekommunikation welche oft in Schnurlostelefonen eingesetzt wird
LoRaWAN	Long Range Wide Area Network, Drahtlos-Netzprotokoll
BSI	Bundesamts für Sicherheit in der Informationstechnik

Versicherung über redliches wissenschaftliches Arbeiten

Hiermit versichere ich, Ben Lutz, dass ich die vorliegende Arbeit selbstständig verfasst und erstellt habe. Ich versichere, dass ich nur zugelassene Hilfsmittel und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ferner versichere ich, dass ich alle wörtlich oder sinngemäß übernommenen Stellen in der Arbeit gemäß gängiger wissenschaftlicher Zitierregeln korrekt zitiert und als solche gekennzeichnet habe. Darüber hinaus versichere ich, dass alle verwendeten Hilfsmittel, wie KI-basierte Chatbots (bspw. ChatGPT), Übersetzungs- (bspw. DeepL), Paraphrasier- (bspw. Quillbot) oder Programmier-Applikationen (bspw. Github Copilot) vollumfänglich deklariert und ihre Verwendung an den entsprechenden Stellen angegeben und gekennzeichnet habe.

Ich bin mir bewusst, dass die Nutzung maschinell generierter Texte keine Garantie für die Qualität von Inhalten und Text gewährleistet. Ich versichere, dass ich mich textgenerierender KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Ich verantworte die Übernahme jeglicher von mir verwendeter maschinell generierter Textpassagen vollumfänglich selbst.

Auch versichere ich, die „Satzung der Hochschule Furtwangen (HFU) zur Sicherung guter wissenschaftlicher Praxis“ vom 27. Oktober 2022 zur Kenntnis genommen zu haben und mich an den dortigen Ausführungen zu orientieren.

Mir ist bewusst, dass meine Arbeit auf die Benutzung nicht zugelassener Hilfsmittel oder Plagiate überprüft werden kann. Auch habe ich zur Kenntnis genommen, dass ein Verstoß gegen § 10 bzw. § 11 Absatz 4 und 5 der Allgemeinen Teile der HFU-SPOen zu einer Bewertung der betroffenen Arbeit mit der Note 5 oder mit «nicht ausreichend» und/oder zum Ausschluss von der Erbringung aller weiteren Prüfungsleistungen führen kann.

Furtwangen, 22.12.2023

Anhang

Anhang A : Fragenkatalog

Hochschule Furtwangen

Fakultät Informatik

Allgemeine Informatik



Fragenkatalog für ein Interview zum Thema:

Bedrohungsanalyse und Gegenmaßnahmen zur Absicherung der IT-Sicherheit gegen kommerzielle Drohnengefahren

Vorgelegt von:

Name: Ben Lutz

Version des Dokuments: 0.3

Kontaktdaten: ben.lutz@hs-furtwangen.de

Datum:

Vorbereitung

- Kurze Vorstellung Ben Lutz
- Vorstellung des Themas, der Forschungsfrage und der ungefähren Dauer
- Kurze Vorstellung des Interviewpartners
- Einwilligung zur Gesprächsaufzeichnung

Interviewfragen

Einführung

- Haben Sie selbst Erfahrungen mit Drohnen gemacht?
- Wie stehen Sie selbst zu Drohnen?

Gefahren

- Wie schätzen Sie das Risiko von Drohnen auf die Datensicherheit von Unternehmen ein?
- Fallen Ihnen Szenarien ein, in denen Drohnen eine direkte Bedrohung für die Datensicherheit eines Unternehmens darstellen?
- Fallen Ihnen Szenarien ein, bei denen Drohnen helfen könnten die Datensicherheit eines Unternehmens zu gefährden (indirekte Gefahren)?
- Wie schätzen Sie die Dunkelziffer bei Angriffen auf die Datensicherheit mit Hilfe von Drohnen ein?

Abwehr

- Wie könnten sich Unternehmen (kosteneffizient) gegen Drohnengefahren schützen?
- Fallen Ihnen bestehende Vorschriften ein, welche die Gefahr von Drohnen auf IT-Sicherheitsrisiken adressieren?
- Welchen Rat würden Sie Unternehmen geben, um in Zukunft potenziellen drohnenbezogenen IT-Sicherheitsbedrohungen einen Schritt voraus zu sein?
- Können Sie einen Vorfall teilen, bei dem Sie oder Ihnen bekannte Personen Erfahrungen mit einem drohnenbezogenen IT-Sicherheitsproblem gemacht haben?

Abschluss

- Wie schätzen Sie die aktuelle und zukünftige Lage der IT-Sicherheit in Bezug auf Drohnengefahren ein?
- Haben Sie weitere Ressourcen / Interviewpartner zu diesem Thema?
- Kurze Zusammenfassung des Interviews

Ende

- Gibt es Passagen, die nicht verwendet werden sollen?
- Möchten Sie über den weiteren Fortschritt informiert werden? Wenn ja, wie?
- Danksagung und Verabschiedung

Anhang B : Datenschutzerklärung



Datenschutzhinweis zur Erhebung, Verarbeitung und Übermittlung personenbezogener Interviewdaten für wissenschaftliche Zwecke

Forschungsprojekt	Bedrohungsanalyse und Gegenmaßnahmen zur Absicherung der IT-Sicherheit gegen kommerzielle Drohnengefahren
Durchführende Institution	Hochschule Furtwangen
Projektleitung	Ben Lutz
Interviewer	Ben Lutz
Interviewdatum	

Die Interviews werden mit einem Aufnahmegerät aufgezeichnet und sodann von den Mitarbeiterinnen und Mitarbeitern des Forschungsprojekts von einem Dienstleister auf Grundlage eines Auftragsdatenvertrages in Schriftform gebracht. Für die weitere wissenschaftliche Auswertung werden die personenbezogenen Kontaktdaten (Namen Vorname, Anschrift ggfls. weitere) von den Interviews getrennt und für Dritte unzugänglich gespeichert. Nach Beendigung des Forschungsprojekts werden Ihre Kontaktdaten gelöscht.

Eine Zugriffsberechtigung auf die Kontaktdaten während der Projektlaufzeit haben nur die Projektleitenden und die im Projekt beschäftigten Personen.

Die Teilnahme an den Interviews ist freiwillig. Sie haben zu jeder Zeit die Möglichkeit, ein Interview abzubrechen, weitere Interviews abzulehnen und Ihr Einverständnis in eine Aufzeichnung und Niederschrift des/der Interviews zurückziehen, ohne dass Ihnen dadurch irgendwelche Nachteile entstehen.

In wissenschaftlichen Veröffentlichungen werden Interviews nur in Ausschnitten zitiert, um gegenüber Dritten sicherzustellen, dass der entstehende Gesamtzusammenhang von Ereignissen nicht zu einer Identifizierung der Person führen kann. Angaben, die zu einer Identifizierung der Person führen können, werden anonymisiert oder aus dem Text entfernt.

Ihre Interviewdaten werden nach Projektabschluss an die Bibliothek der Hochschule Furtwangen zur Archivierung und weiteren wissenschaftlichen Nutzung übermittelt. Das Archiv stellt Wissenschaftlerinnen und Wissenschaftlern die Interviewdaten für ausschließlich wissenschaftliche Forschungszwecke zur Verfügung.

Eine Übermittlung Ihrer personenbezogenen Daten nach außerhalb des Europäischen Wirtschaftsraumes ist nicht geplant.

Unter den in der DSGVO genannten Voraussetzungen haben Sie folgende Datenschutzrechte:

Sie haben das Recht, Auskunft darüber zu verlangen, welche personenbezogenen Daten und welche Kategorie personenbezogener Daten von Ihnen verarbeitet werden, zu welchem Zweck dies geschieht, an welche Empfänger Ihre personenbezogenen Daten übermittelt wurden und über die geplante Dauer der Verarbeitung Ihrer personenbezogenen Daten. Außerdem haben Sie ein Recht, auf die Übertragung Ihrer Daten.

Sie können beim Verantwortlichen (s.o.) jederzeit Ihr Recht auf Berichtigung oder Löschung der Sie betreffenden personenbezogenen Daten geltend machen und/oder beim Verantwortlichen der Verarbeitung Ihrer personenbezogenen Daten widersprechen oder diese einschränken.



Außerdem haben Sie das Recht, die von Ihnen erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen zu können, ohne dass Ihnen dadurch irgendwelche Nachteile entstehen.

Ihnen steht das Recht auf Beschwerde bei einer Aufsichtsbehörde insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, zu, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt.

EINWILLIGUNGSERKLÄRUNG

In Kenntnis der vorstehenden Hinweise, die ich gelesen und verstanden habe, willige ich in die in dem Hinweis genannten Verarbeitungen meiner personenbezogenen Daten, einschließlich besonderer Kategorien von Daten im Rahmen des genannten Forschungsprojekts ein und bin deshalb bereit, an einem Interview/ an mehreren Interviews teilzunehmen.

Mir ist bekannt, dass ich diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann, ohne dass ich Nachteile dadurch haben werde. Den Widerruf kann ich schriftlich oder per E-Mail datenschutz@hfu.eu erklären.

ja

nein

Vorname; Nachname in Druckschrift

Ort, Datum / Unterschrift

Anhang C : Kodierleitfaden

Kategorie	Definition	Ankerbeispiel	Kodierregel
K1: Gefahren			
<i>K1.1: Indirekte Gefahren</i>	Indirekte Bedrohungen auf die Informationssicherheit mit Hilfe von Drohnen	„Also es gibt tagesaktuelle Bilder, klar, das ist ein Punkt, der valide ist.“ (12, Pos.8)	Bedrohungen welche bei erfolgreicher Durchführung Vorteile für weitere Angriffe bieten
<i>K1.2: Direkte Gefahren</i>	Direkte Bedrohungen auf die Informationssicherheit mit Hilfe von Drohnen	„Es gibt offensichtlich mittlerweile Angriffsszenarien, wo auf IoT Systeme durch den Überflug einer Drohne, die dann über ihr [...] über WLAN oder Bluetooth bestimmte Impulse sendet, ja Angriffe ausgelöst werden.“ (14, Pos. 6)	Bedrohungen welche bei erfolgreicher Durchführung sofort die Informationssicherheit verletzen
<i>K1.3: Machbarkeit von Angriffen</i>	Aussagen über die Schwierigkeit und Praktikabilität von Drohnenbezogene Angriffen auf die Informationssicherheit	„Das ist relativ leicht machbar, wenn man ein bisschen Hintergrundkenntnisse hat, so Software Defined Ratio bisschen machen kann, dann denke ich, kann man [solch einen Angriff] umsetzen“ (15, Pos. 33)	Aussagen über Komplexität von Angriffen oder über die sowohl positive als auch negative Umsetzungswahrscheinlichkeit dieser in der Realität
K2: Abwehr			
<i>K2.1: Abwehr Möglichkeiten</i>	Aussagen über Möglichkeiten bei der Abwehr von Drohnen	„Ansonsten gibt es noch die Möglichkeit, die irgendwie abzuschießen, mit einem Fangnetz oder mit einer Gegendrohne dagegen zu fliegen, dass sie runter fliegt.“ (12, Pos. 25)	Beschreibungen technischer oder organisatorischer Maßnahmen zur Abwehr von Drohnen

Kategorie	Definition	Ankerbeispiel	Kodierregel
<i>K2.2: Abwehr Herausforderungen</i>	Herausforderungen im Bereich der Drohnenabwehr	<i>„[Der Einsatz von destruktiven Maßnahmen zur Drohnenabwehr] ist natürlich sehr umstritten auch vor allem, wenn das dann außerhalb des Werksgelände ist, ob es dann Sachbeschädigung ist usw.“ (14, Pos. 11)</i>	Aussagen über jeglichen Problematiken oder Einschränkungen die sich bei der Abwehr von Drohnen ergeben
K3: Aktuelle Lage			
<i>K3.1: Präsenz im Fachgebiet</i>	Diskussionen zum untersuchten Thema im Arbeitsalltag der Interviewpartner	<i>„in meinem aktuellen Arbeitsumfeld wird es Thema. Wenig bis kaum behandelt, wenn ich meine Arbeit ausklammere.“ (11, Pos. 50)</i>	Jegliche Aussagen über den Diskurs zum Thema Drohnen im Kontext der Informationssicherheit
<i>K3.2: aktuelle Gefährdungslage</i>	Einschätzung der aktuellen Bedrohungslage durch Drohnen auf die Informationssicherheit	<i>„Also die aktuelle Lage sehe ich. Um es mal vielleicht zu benennen, eher als Medium an, was IT Security betrifft in Bezug zu Drohnen.“ (12, Pos. 42)</i>	Konkrete Einschätzungen der untersuchten Gefahrenlage

Anhang D : Referenzblatt mit fiktiven sensiblen Informationen

Hinweis: Der Maßstab des Anhangs entspricht nicht dem des tatsächlich im Experiment genutzten und illustriert lediglich die Darstellung der fiktiven Daten.

72 **Unsere Firma
expandiert in
internationale
Märkte.**

48 **Der Kundenservice ist
von 9 bis 17 Uhr
erreichbar.**

36 **Wir suchen nach neuen
Mitarbeitern für das Team.**

28 **Das Budget für das Projekt wurde
genehmigt.**

16 **Bitte bestätigen Sie Ihre Anwesenheit beim Workshop.**

13 **Die Lieferung wurde heute versandt, Ankunft am Dienstag.**

12 **Wir benötigen Ihre Unterschrift für den Vertrag.**

Anhang E : Exemplarische Versuchsfragen

1. Technische Sicherheit

- a. **Zuverlässigkeit der Hardware:** Wie robust ist die Drohnentechnologie gegenüber physischen Störungen und Ausfällen?
- b. **Software-Integrität:** Welche Maßnahmen werden ergriffen, um die Software vor unerlaubtem Eingriff und Fehlfunktionen zu schützen?
- c. **Kommunikationssicherheit:** Wie wird die sichere Übertragung von Steuerbefehlen und Daten gewährleistet?

2. Regulatorische und Compliance-Aspekte

- a. **Gesetzliche Vorschriften:** Welchen gesetzlichen Bestimmungen unterliegt der Betrieb von Drohnen in verschiedenen Lufträumen?
- b. **Datenschutz:** Wie werden die Datenschutzbestimmungen bei der Aufnahme und Speicherung von Daten eingehalten?
- c. **Flugverbotszonen:** Wie wird sichergestellt, dass Drohnen keine Flugverbotszonen betreten?

3. Ethische und Privacy-Überlegungen

- a. **Überwachung und Privatsphäre:** Wie wird verhindert, dass Drohnen zur unerlaubten Überwachung eingesetzt werden?
- b. **Auswirkungen auf die Öffentlichkeit:** Welche Maßnahmen werden ergriffen, um die Auswirkungen des Drohnenbetriebs auf die Allgemeinheit zu minimieren?

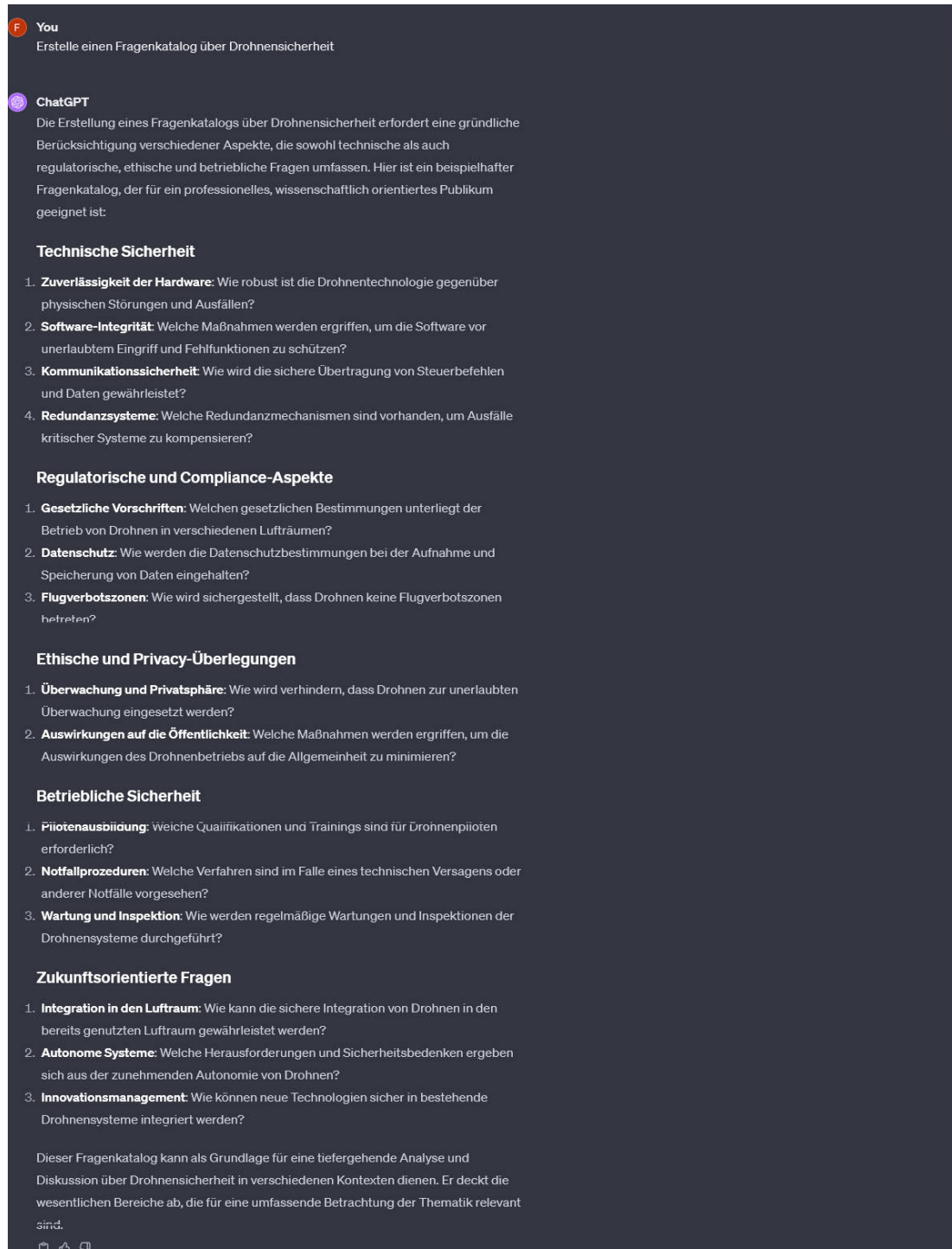
4. Betriebliche Sicherheit

- a. **Pilotenausbildung:** Welche Qualifikationen und Trainings sind für Drohnenpiloten erforderlich?
- b. **Notfallprozeduren:** Welche Verfahren sind im Falle eines technischen Versagens oder anderer Notfälle vorgesehen?
- c. **Wartung und Inspektion:** Wie werden regelmäßige Wartungen und Inspektionen der Drohnensysteme durchgeführt?

5. Zukunftsorientierte Fragen

- a. **Integration in den Luftraum:** Wie kann die sichere Integration von Drohnen in den bereits genutzten Luftraum gewährleistet werden?
- b. **Autonome Systeme:** Welche Herausforderungen und Sicherheitsbedenken ergeben sich aus der zunehmenden Autonomie von Drohnen?
- c. **Innovationsmanagement:** Wie können neue Technologien sicher in bestehende Drohnensysteme integriert werden?

Anhang F : Screenshot der Fragenkatalog KI-Konversation



You
Erstelle einen Fragenkatalog über Drohnensicherheit

ChatGPT
Die Erstellung eines Fragenkatalogs über Drohnensicherheit erfordert eine gründliche Berücksichtigung verschiedener Aspekte, die sowohl technische als auch regulatorische, ethische und betriebliche Fragen umfassen. Hier ist ein beispielhafter Fragenkatalog, der für ein professionelles, wissenschaftlich orientiertes Publikum geeignet ist:

Technische Sicherheit

- Zuverlässigkeit der Hardware:** Wie robust ist die Drohnentechnologie gegenüber physischen Störungen und Ausfällen?
- Software-Integrität:** Welche Maßnahmen werden ergriffen, um die Software vor unerlaubtem Eingriff und Fehlfunktionen zu schützen?
- Kommunikationssicherheit:** Wie wird die sichere Übertragung von Steuerbefehlen und Daten gewährleistet?
- Redundanzsysteme:** Welche Redundanzmechanismen sind vorhanden, um Ausfälle kritischer Systeme zu kompensieren?

Regulatorische und Compliance-Aspekte

- Gesetzliche Vorschriften:** Welchen gesetzlichen Bestimmungen unterliegt der Betrieb von Drohnen in verschiedenen Lufträumen?
- Datenschutz:** Wie werden die Datenschutzbestimmungen bei der Aufnahme und Speicherung von Daten eingehalten?
- Flugverbotszonen:** Wie wird sichergestellt, dass Drohnen keine Flugverbotszonen betreten?

Ethische und Privacy-Überlegungen

- Überwachung und Privatsphäre:** Wie wird verhindert, dass Drohnen zur unerlaubten Überwachung eingesetzt werden?
- Auswirkungen auf die Öffentlichkeit:** Welche Maßnahmen werden ergriffen, um die Auswirkungen des Drohnenbetriebs auf die Allgemeinheit zu minimieren?

Betriebliche Sicherheit

- Pilotenausbildung:** Welche Qualifikationen und Trainings sind für Drohnenpiloten erforderlich?
- Notfallprozeduren:** Welche Verfahren sind im Falle eines technischen Versagens oder anderer Notfälle vorgesehen?
- Wartung und Inspektion:** Wie werden regelmäßige Wartungen und Inspektionen der Drohnensysteme durchgeführt?

Zukunftsorientierte Fragen

- Integration in den Luftraum:** Wie kann die sichere Integration von Drohnen in den bereits genutzten Luftraum gewährleistet werden?
- Autonome Systeme:** Welche Herausforderungen und Sicherheitsbedenken ergeben sich aus der zunehmenden Autonomie von Drohnen?
- Innovationsmanagement:** Wie können neue Technologien sicher in bestehende Drohnensysteme integriert werden?

Dieser Fragenkatalog kann als Grundlage für eine tiefere Analyse und Diskussion über Drohnensicherheit in verschiedenen Kontexten dienen. Er deckt die wesentlichen Bereiche ab, die für eine umfassende Betrachtung der Thematik relevant sind.

📄 🔄 🔗

Anhang G : Monatsberichte

Fakultät Informatik

Thesis-Seminar im Bachelor-Studium – monatliche Berichterstattung

Berichtszeitraum: November 2023

Thema der Thesis:	Bedrohungsanalyse und Gegenmaßnahmen zur Absicherung der IT-Sicherheit gegen kommerzielle Drohnengefahren
Bearbeiter/in:	Ben Lutz
Kontakt:	ben.lutz@hs-furtwangen.de / [REDACTED]

Durchgeführte Arbeiten (13-15 Zeilen)

Wie zuvor für den aktuellen Berichtszeitraum geplant, fokussierten sich die Arbeiten in diesem Monat auf die inhaltliche Analyse der Experteninterviews. Hierzu wurden zu Beginn des Monats drei weitere Interviews geführt und transkribiert. Dies bringt die insgesamt Zahl der Interviews auf sechs. Da alle weiteren Interviewanfragen verliefen, schließt dies den Teil der Interviews. Nach der vollständigen Transkription der Interviews wurden die Inhalte aus knapp vier Stunden Interview Material analysiert. Die Erkenntnisse aus den Interviews flossen vor allem in den Teil der Gefahrenanalyse ein. Auch kritische Expertenmeinungen wurden erfasst und erweitern die Gefahrenanalyse um eine allgemeine Differenzierung. Neben dem Teil der Gefahren wurde auch der Teil der Abwehrmaßnahmen in großen Teilen vervollständigt. Hierzu wurde eine weitere grundlegende Literaturrecherche durchgeführt. Außerdem wurde der praktische Versuch durchgeführt und dokumentiert.

Erzielte Ergebnisse (8-10 Zeilen)

Das signifikanteste Ergebnis ist die Fertigstellung der Interviewanalyse. Das Wissen der Experten floss in viele Teile der Arbeit ein. Unter anderem auch dem Teil der Abwehrmaßnahmen welcher ebenfalls weitestgehend erstellt wurde. So konnte im Rahmen dessen einige Maßnahmen identifiziert werden, welche von der Literatur nicht erwähnt wurden. Auch die Durchführung des praktischen Versuchs ermöglichte die Fertigstellung einiger Kapitel, welche auf den dadurch gewonnenen Erkenntnissen basierten.

Abweichungen / Probleme (6-8 Zeilen)

Mit den Erkenntnissen aus den Interviews, der Abwehnanalyse und einer ersten Korrektur des Zweitbetreuers wurde die Struktur der Arbeit stark abgeändert. Die neue Struktur weist eine bessere Nachvollziehbarkeit durch Fusion und Neuordnung von Unterkapiteln auf. Außerdem wurden Redundanzen eliminiert und die Methoden jeweils in den praktischen Kapiteln gekapselt, um einen besseren Lesefluss zu ermöglichen. Signifikante Probleme gab es nicht.

Ausblick über die geplanten Tätigkeiten und Ergebnisse des nächsten Berichtszeitraums (4-6 Zeilen)

Der letzte Monat der Arbeit konzentriert sich auf die Fertigstellung der Kapitel und die Korrektur. Zusammenfassende Kapitel sowie die Diskussion sind noch offen und bilden den Abschluss der Arbeit. Die Anpassung des Titels ist ebenfalls geplant um die gewonnenen Erkenntnisse besser zu repräsentieren. Nach Abschluss dieses Berichtszeitraums wird die Arbeit voraussichtlich fertiggestellt.

Fakultät Informatik

Thesis-Seminar im Bachelor-Studium – monatliche Berichterstattung

Berichtszeitraum: Oktober 2023

Thema der Thesis:	Bedrohungsanalyse und Gegenmaßnahmen zur Absicherung der IT-Sicherheit gegen kommerzielle Drohnengefahren
Bearbeiter/in:	Ben Lutz
Kontakt:	ben.lutz@hs-furtwangen.de / [REDACTED]

Durchgeführte Arbeiten (13-15 Zeilen)

Wie im vergangenen Bericht geplant, fokussierten sich die Arbeiten in diesem Monat auf die Experteninterviews. Insbesondere wurden drei Interviews durchgeführt und transkribiert. Aufgrund der geringen Antwortrate der Angefragten Partner, wurden weitere Partner angefragt. Darunter sind Firmen wie Rohde & Schwarz, Kaspersky und PwC. Resultierend aus den Anfragen wurden zwei weitere Interviews terminiert. Ebenfalls wurden Fortschritte im Teil der Interviews gemacht. Diese bestehen aus dem Einlesen in diverse Vorgehensweisen für die strukturierte Analyse der gesprochenen Inhalte. In Fall der Arbeit wird die Vorgehensweise der Qualitativen Inhaltsanalyse nach Mayring angewendet.

Erzielte Ergebnisse (8-10 Zeilen)

Konkret wurde der Teil der Literaturrecherche abgeschlossen. Mit dem Abschluss dieses Teil ist ein großer Teil der theoretischen Arbeit erledigt und es können die praktischeren Teile des Versuchs sowie den Interviews angegangen werden. Ein weiteres messbares Ergebnis sind die bereits transkribierten Inhalte der Interviews. Zusammen mit Zeitstempeln ist hier ein Inhalt von ca. 68 Seiten entstanden der nun analysiert werden kann.

Abweichungen / Probleme (6-8 Zeilen)

Im Vergleich zum letzten Monat gab es wenige Abweichungen. Während der Durchführung der Interviews wurde an einigen Stellen klar, dass die Gefahren, welche von Drohnen ausgehen, doch nicht so gravierend sind wie angenommen. Hiervon geht keine konkrete Abweichung aus, dieser Fakt unterscheidet sich jedoch vom erwarteten Ergebnis. Bezüglich des Teils der Konkreten Zwischenfälle gibt es Überlegungen diesen umzuwandeln oder zu streichen. Grund dafür ist die spärliche Lage von öffentlich bekannten Zwischenfällen. Auch alle bisherigen Interviewpartner können aufgrund der Abstinenz der Vorfälle oder des Datenschutzes keine weiteren Vorfälle nennen. Im Falle einer Umgestaltung des Teils könnte man den Informationssicherheitsfokus erweitern und Drohnenzwischenfälle allgemein analysieren.

Ausblick über die geplanten Tätigkeiten und Ergebnisse des nächsten Berichtszeitraums (4-6 Zeilen)

Der kommende Monat sollen die geführten Interviews analysiert werden. Mit der Fertigstellung dieses Teil würde der Teil der Gefahrenanalyse komplett abgeschlossen sein. Dieser Abschluss markiert ungefähr 60-65% der Arbeit. Außerdem soll der praktische Teil durchgeführt und dokumentiert werden. Mit der Erreichung dieser beiden Ziele kann sich auf die Abwehrmaßnahmen, der abschließenden Diskussion und dem „Feinschliff“ befasst werden.

Fakultät Informatik

Thesis-Seminar im Bachelor-Studium – monatliche Berichterstattung

Berichtszeitraum: September 2023

Thema der Thesis:	Bedrohungsanalyse und Gegenmaßnahmen zur Absicherung der IT-Sicherheit gegen kommerzielle Drohnengefahren
Bearbeiter/in:	Ben Lutz
Kontakt:	ben.lutz@hs-furtwangen.de / [REDACTED]

Durchgeführte Arbeiten (13-15 Zeilen)

Im vergangenen Monat lag der Fokus maßgeblich auf der Literaturrecherche und der Vorbereitung qualitativer Interviews. Dabei wurden umfassende Recherchen zu den Themen Drohnen, dem aktuellen Stand der Technik und IT-Sicherheit durchgeführt. Parallel dazu wurden verwandte wissenschaftliche Arbeiten und potenzielle Angriffsvektoren aus der Literatur untersucht, um ein Bild der Thematik zu erhalten. Ein weiterer wichtiger Schritt war die Begehung der Rechenzentren der BadenIT. Diese diente als Inspiration für mögliche Angriffe und regte Überlegungen zur Umgestaltung des Praktischen Teils an. Des Weiteren half der Austausch mit zwei Kollegen der BadenIT dabei einen Eindruck von Stand der Lage in Bezug auf Awareness und Drohnenabwehr zu bekommen. Im Zuge der Interviewvorbereitung wurden auch Überlegungen zu den inhaltlich relevanten Fragen angestellt und Datenschutzbestimmungen für die Durchführung der Interviews recherchiert. Schließlich konnten neun Interviewpartner identifiziert und für die Teilnahme an den bevorstehenden Interviews angefragt werden. Diese Maßnahmen stellen einen wichtigen Grundstein für die weiterführende Forschungsarbeit dar.

Erzielte Ergebnisse (8-10 Zeilen)

Die erzielten Ergebnisse des vergangenen Monats setzen sich aus verschiedenen Komponenten zusammen. Es wurden mehrere Kapitel für den Forschungsbericht verfasst, darunter die Einleitung, ein Überblick über verwandte Arbeiten, eine generelle Betrachtung von Drohnen sowie der aktuelle Stand der Technik in diesem Bereich. Zusätzlich wurde ein Kapitel zur Literaturrecherche über potenzielle Angriffe angefangen. Im Hinblick auf die qualitative Datenerhebung wurde ein Fragenkatalog für die Interviews erarbeitet und eine Datenschutzerklärung formuliert. Erfreulicherweise haben bereits zwei Interviewpartner ihre Teilnahme zugesagt, während sechs weitere Anfragen noch ausstehen.

Abweichungen / Probleme (6-8 Zeilen)

Abweichungen gab es vor allem im Bereich des Praktischen Teils. Die Begehung der Rechenzentren stellte heraus das sich diese aufgrund ihrer besonderen Absicherung nicht als besten Ort für einen Praxisversuch eignen. Stattdessen wird der praktische Teil nun in einem weniger abgesicherten Bereich wie z.B. Nutzerendpunkten durchgeführt. Der Bereich der Gefahrenanalyse wurde ebenfalls etwas gekürzt. Der ursprüngliche Versuch „alle“ Gefahren zu identifizieren ist unrealistisch. Stattdessen wird versucht einige Angriffe mit einer hohen Eintrittswahrscheinlichkeit zu identifizieren und die Liste der Gefahren Exemplarisch zu halten. Dadurch kann der Umfang auch um einen kurzen Teil über die Drohnenabwehr erweitert werden.

Ausblick über die geplanten Tätigkeiten und Ergebnisse des nächsten Berichtszeitraums (4-6 Zeilen)

Der kommende Monat wird sich vor allem auf die Experteninterviews konzentrieren. Insbesondere auf die Terminierung, Durchführung, Transkription und anschließende Analyse. Außerdem soll der Teil der Literaturrecherche in Bezug auf Gefahren fertiggestellt und der Teil der Analyse von realen Zwischenfällen vollständig erstellt werden. Dies würde den Teil der Gefahrenanalyse abschließen, so dass im November mit dem praktischen Teil sowie mit den Abwehrmaßnahmen gegen diesen begonnen werden kann.

Fakultät Informatik

Thesis-Seminar im Bachelor-Studium – monatliche Berichterstattung

Berichtszeitraum: Dezember 2023

Thema der Thesis:	Bedrohung von oben: Analyse des Gefahrenpotenzials von frei erhältlichen Drohnen für die Informationssicherheit von Unternehmen
Bearbeiter/in:	Ben Lutz
Kontakt:	ben.lutz@hs-furtwangen.de / [REDACTED]

Durchgeführte Arbeiten (13-15 Zeilen)

Wie zuvor für den aktuellen Berichtszeitraum geplant, fokussierten sich die Arbeiten in diesem Monat auf die Fertigstellung der noch offenen Kapitel sowie die Korrektur der Inhalte. Hierzu wurden die Kapitel der Diskussion und des Fazits erstellt. Außerdem wurde die Arbeit am 15 Korrekturleser verteilt. Korrekturen wurden kontinuierlich in die endgültige Fassung der Arbeit eingearbeitet. Des Weiteren wurden verschiedene Teile der Arbeit überarbeitet und umstrukturiert. Außerdem wurde der Titel angepasst, um die Forschung der Arbeit prägnanter und treffender zusammenzufassen.

Erzielte Ergebnisse (8-10 Zeilen)

Mithilfe der zahlreichen Anmerkungen der Korrektur Leser konnte der Inhalt die Formatierung und die Struktur der Arbeit weiter verbessert werden. Der Titel beschreibt nun ebenfalls besser das Forschungsziel. Mit der Fertigstellung der Kapitel und der Korrektur stellt dies den Abschluss der Thesis da. Die Arbeit wird außerdem für das Programm des 20. Deutschen IT-Sicherheitskongresses des Bundesamts für Sicherheit in der Informationstechnik angenommen.

Abweichungen / Probleme (6-8 Zeilen)

Die Abweichungen in diesem Berichtszeitraum beziehen sich hauptsächlich auf zahlreiche kleine grammatikalische und inhaltliche Änderungen innerhalb der Abschnitte. Außerdem wurde der Titel der Arbeit angepasst. Auch wurde eine Reihe an förmlichen Änderungen vorgenommen, um die Leserlichkeit der Arbeit zu verbessern. Signifikante, ungeplante Änderungen in der Struktur oder im Inhalt gab es nicht.

Ausblick über die geplanten Tätigkeiten und Ergebnisse des nächsten Berichtszeitraums (4-6 Zeilen)

Dieser Bericht beschreibt den letzten Berichtszeitraum dieser Arbeit.