# Scenario Analysis of Threats Posed to Critical Infrastructures by Civilian Drones

Moritz Schneider

*Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany. E-mail: moritz.schneider@dlr.de*

Daniel Lichte

*Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany. E-mail: daniel.lichte@dlr.de*

Dustin Witte

*Institute for Security Systems, University of Wuppertal, Germany. E-mail: witte@uni-wuppertal.de*

Stephan Gimbel

*Department of Computer Science, University of Applied Sciences Darmstadt, Germany. E-mail: stephan.gimbel@h-da.de*

Eva Brucherseifer

*Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center (DLR), Germany. E-mail: eva.brucherseifer@dlr.de*

Threats posed by civilian drones are becoming an increasing security risk for critical infrastructures as well as events or companies. In order to protect an asset against a drone intrusion a security system is necessary, which in general is described by its capabilities of protection, detection, and intervention. The variety of different threat scenarios posed by drones raises the need for detailed analysis of scenario specific requirements on detection systems. However, there is a lack of comprehensive scenario analyses in the literature that include relevant parameters for detection. Thus, in this paper a scenario analysis is conducted to identify consistent threat scenarios including factors critical for drone detection. The study is based on morphological analysis and applies methods of influence analysis and Cross-Impact Balance analysis. Using these methods, factors that influence the detectability of drones are specified and key factors identified. Potential states of these key factors are determined based on literature reviews or expert interviews. For the assessment of internal consistency of a scenario, a Cross-Impact-Balance analysis is conducted. Exemplarily, the paper shows how a remaining consistent scenario can be applied to derive requirements for a drone detection system or to validate existing systems regarding suitability for feasible threat scenarios.

*Keywords*: Critical Infrastructure Protection, Security, Civilian Drones, Scenario Analysis, Morphological Analysis, Cross-Impact Analysis, UAV, Requirements Analysis, Drone Detection System.

## 1. Introduction

The number and variety of civilian drones is constantly increasing due to the rapid technological development. While in the past the airspace was dominated by commercial air traffic, drones are mostly used by individuals leading to an increasing total amount of flying objects in airspace. Supporting this effect, the development of autonomously flying drones opens up potential for various use cases, e.g. in the context of parcel transport (Bamburry, 2015; Murray and Chu, 2015; Stolaroff et al., 2018). However, these developments also increase the threats posed by civilian drones, as they open up opportunities for criminal and terrorist activities. For example, drones can be used for industry espionage or to disrupt air traffic at airports, which can lead to high financial losses (Wendt et al., 2020). Thus, it is necessary to protect critical infrastructures as well as companies and events against attacks by civilian drones. In order to protect an asset against a drone attack, security systems specialized for this threat are essential. These in general can be categorized based on their capabilities of protection, detection and intervention (Garcia, 2017). Preventing drone flights in critical areas as well as the intervention in case of unwanted drone intrusion is complex, costly, or even impossible. This increases the need for reliable drone detec-

*Proceedings of the 31st European Safety and Reliability Conference*
*Edited by* Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
*Published by* Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_234-cd

tion. Various detection systems based on different technologies, e.g. radar, acoustic, visual or radiofrequency, are already available on the market. These technologies show different strengths and weaknesses, which strongly depend on different factors, such as weather conditions or type of drone control (see Taha and Shoufan (2019)). Therefore, a scenario-dependent evaluation of a detection system is beneficial. In addition, analyzing specific scenarios can help to identify suitable detection systems.

Thus, in this paper, a scenario analysis is conducted to identify consistent threat scenarios posed by civilian drones. In addition to the intent of the attacker and the asset being threatened, the scenarios contain parameters relevant for drone detection. Common methodologies for scenario analysis and consistency evaluation of the scenarios are applied. The results of this analysis can be used to derive scenario specific requirements for a detection system. This supports the identification of suitable detection systems for certain scenarios or use cases of certain detection systems.

## 2. Methods

### 2.1. *Morphological analysis*

The morphological analysis represents a structured method for the development of relevant and consistent scenarios (Johansen, 2018). Within the analysis, influencing factors concerning the question of interest are collected. These factors can be considered as dimensions of uncertainties of the scenario, whereas the states of these factors can be defined as possible characteristics of these uncertainties. Thus, the influencing factors form the dimensions of the scenario space containing all possible combinations of factor states. Literature reviews as well as expert interviews can serve as a source to identify these factors and their states (Johansen, 2018; Ritchey, 2012). The morphological analysis is used in several contexts, such as threat analysis, product design or studies concerning future developments (see Alvarez and Ritchey (2012) for an overview of topics). Thus, a scenario is defined as a combination of a certain state of each considered factor.

### 2.2. *Influence analysis*

Based on the influence analysis, factors can be identified that show a high or low level of interconnectedness within the scenario space. Therefore, factors are evaluated pairwise in the influence matrix concerning their directed influence. The matrix is set up by the juxtaposition of all factors. Due to the directional evaluation, it can be an asymmetric matrix, since factor $A$ can have an influence on factor $B$, but $B$ might not have an influence on $A$. The size of the matrix increases in square as the number of factors increases. For n factors, it is thus an $n \times n$ matrix. The influence assessment within the matrix can be based on a binary scale (1 = influence, 0 = no influence) or on a multilevel scale that describes nominally different degrees of influence (see Gausemeier et al. (1996)). As a result of the influence analysis, the level of interconnectedness of each factor can be assessed by calculating active and passive sum of the factor values in the matrix (Gausemeier and Plass, 2014). The active sum describes one factor's influence on the other factors. The passive sum, on the other hand, describes how many factors influence that factor (Gausemeier et al., 1996). As a result, factors without relevant influence on the scenario, i.e. factors with insufficient active or passive sum, can be excluded from further analysis. The remaining factors are referred to as key factors. This process reduces the scenario space and therefore the complexity of the following analysis. Furthermore, the results can be used to identify factors for scenario clustering.

### 2.3. *Cross-Impact Balance analysis*

The Cross-Impact Balance analysis (CIB) serves as a method to identify consistent scenarios within the scenario space. The scenario space contains all possible combinations of the factor states, whereby states can also be mutually exclusive because of logical or functional aspects and thus form inconsistent scenarios. In the CIB, the states of the key factors are checked pairwise with regard to their consistency (conclusiveness) of joint occurrence. Therefore, the CIB Matrix is set up, representing a structured means to conduct the pairwise assessment. The matrix is set up by the juxtaposition of all factor states. Thus, the size of the matrix grows in square with the number of considered states. The consistency assessment of two states is performed by means of a multilevel scale (Weimer-Jehle, 2006). Thereby, the scale can vary depending on the desired level of detail. Impact balances are created, which can be used to identify consistent state bundles. All possible scenarios are systematically checked for overall consistency. Nash equilibria are searched for, whereby the consistency condition is fulfilled if the exchange of a state can not lead to a higher consistency value in the impact balance (Weimer-Jehle, 2006).

## 3. Scenario Development

The first step for developing a scenario is the identification of the specific object of the analysis (Johansen, 2018). In this case, the objective of the scenario analysis is to identify threat scenarios posed by civilian drones, including factors relevant for drone detection. The scenarios are intended to be exploratory and thus should include

all possible states of a factor, regardless of their probability of occurrence (Bishop et al., 2007). It should be noted that only available drone technology is considered within the scenario analysis.

### 3.1. *Scenario space*

To determine the scenario space, it is important to consider an initial structure that supports the definition and classification of relevant factors. According to Garcia (2017), a threat is defined via the *intentions* and the *capabilities* of the adversary. Furthermore, the *asset* at risk and the *tactic* of the attack represent important key properties concerning the threat posed by civilian drones. In sum, there are four characteristic areas in this context, on which the scenarios should provide information and which therefore form the initial outline structure as shown in Fig. 1. In addition, the category *capabilities* of the adversary can be further divided into *drone properties* and *number of drones*. The category referring to the *asset* is subdivided into *asset* and *surroundings*. Based on this, factors describing the categories named above were identified by means of literature reviews and expert interviews. As a result, the influencing factors of the scenario analysis were determined.

Specific sources are indicated for factors derived with the help of literature, whereas the remaining factors were chosen based on expert interviews. In total, 20 factors were identified. Figure 1 shows the assignment of the factors to the previously mentioned outline structure. An overview of all factors and their states is shown in Table 1. As a result, the following detailed descriptions of factors and related states were elaborated:

(1.) *Approach pattern*: includes the pattern in which the drone is flying towards the target as an important part of the attack tactics. The considered patterns are straight line, zigzag path, with or without outbreaks from the sensor area, and circling (Case et al., 2008).

(2.) *Approach distance horizontal*: describes the horizontal distance of the drone between the starting point and the target. The states of this factor describe possible approach distances between $0.1\,\mathrm{km}$ and $10\,\mathrm{km}$.

(3.) *Vertical approach altitude*: describes the altitude of the drone when approaching the asset. The states of this factor describe possible approach altitudes between $0.1\,\mathrm{km}$ and $5\,\mathrm{km}$.

(4.) *Multiple angles of attack*: characterizes whether or not multiple drones are approaching the asset from multiple angles.

(5.) *Jammer*: describes whether or not a jamming signal is used by the attacker to mask the drone.

(6.) *Intent*: refers to the specific intention of the attacker. The states of this factor and thus possible intentions of the attack are summarized in the following options: terrorist attack (Altawy and Youssef, 2017; Valente and Cardenas, 2017), CBRN attack (Altawy and Youssef, 2017; Valente and Cardenas, 2017), jamming (Altawy and Youssef, 2017; Guvenc et al., 2018; Vattapparamban et al., 2016), spoofing (Altawy and Youssef, 2017; Guvenc et al., 2018; Vattapparamban et al., 2016), espionage (Altawy and Youssef, 2017; Valente and Cardenas, 2017) and smuggling (Altawy and Youssef, 2017).

(7.) *Speed of the drone*: describes the speed, at which the drone is flying towards the asset. The states of the factor correspond to average maximum speed of different drone classes.

(8.) *Drone control*: refers to the technology used to control the drone. Possible technologies and thus states are full autonomous control, remote supervised control and remote pilot control (Altawy and Youssef, 2017).

(9.) *Propulsion technology*: refers to the drive system of the drone. Rotary Wing, Fixed Wing and Flapping Wing represent the states of this factor (Floreano and Wood, 2015; Hassanalian and Abdelkefi, 2017).

(10.) *Span of the drone*: describes the length of the spread wing tips or rotors of the drone. Possible spans between $0.1\,\mathrm{m}$ and $2\,\mathrm{m}$ are the states of this factor, since the average span of different types of drones are represented in this range (Hassanalian and Abdelkefi, 2017).

(11.) *Load capacity of the drone*: records the maximum weight load of the drone, which varies in a range from $1\,\mathrm{kg}$ to $10\,\mathrm{kg}$.

(12.) *Drone design*: refers to the design of the drone concerning the size of the reflective plane on the drone. The design can be filigree (no large reflective planes) or compact (dense structure with large reflective planes).

(13.) *Stealth technology*: describes whether or not the drone contains stealth technology that protects from detection by radar technology.

(14.) *Number of drones*: the states of this factor refer to the presence of a single drone or a swarm of drones that includes at least two drones.

(15.) *Asset*: refers to potential attack targets that are threatened by the drone attack. Considered attack targets and thus states of this factor are events, companies and critical infrastructures according to the definition of the German Federal Office of Civil Protection and Disaster Assistance (BBK, 2021).

(16.) *Surrounding settlement*: takes the settlement conditions around the asset into account. The factor is divided into dense settlement (urban area), light settlement (suburban area), rural area and industrial areas.

(17.) *Vegetation*: refers to the presence of vegetation around or on the terrain of the asset to

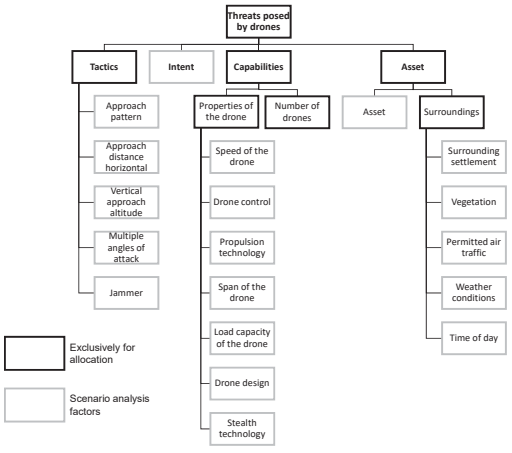


Fig. 1. Outline Structure and Factors

Table 1. Morphological Box of the Analysis

| **Factors** | **States** |
|---|---|
| Approach pattern | straight line, zig-zag path, zig-zag path with outbreaks from the sensor area, circling |
| Approach distance | 0.1 km, 0.2 km, 0.5 km, 1 km, 5 km, 10 km |
| Vertical approach altitude | 0.1 km, 0.2 km, 0.5 km, 1 km, 5 km |
| Multiple angles of attack | yes, no |
| Jammer | comes into use, is not used |
| Intent | terrorist-attack, CBRN-attack, jamming, spoofing, espionage, smuggling |
| Speed of the drone | 35 km/h, 70 km/h, 150 km/h |
| Drone control | full autonomous control, remote supervised control, remote pilot control |
| Propulsion technology | rotary wing, fixed wing, flapping wing |
| Span of the drone | 0.1 m, 0.2 m, 0.5 m, 1 m, 2 m |
| Load capacity of the drone | 1 kg, 5 kg, 10 kg |
| Drone design | no large reflective planes, dense structure with large reflective planes |
| Stealth technology | yes, no |
| Number of drones | single drone, swarm of drones |
| Asset | event, company, research insitute, electricity, gas, mineral oil, district heating, medical care, medicines and vaccines, laboratories, government, parliament, justice institutions, emergency and rescue services, food industry, food trade, aviation, maratime navigation, inland navigation, rail transport, road transport, logistics, banks, stock exchanges, insurances, financial service provider, telecommunications, information technology, broadcast, press, cultural asset, symbolic buildings, public water supply, public wastewater disposal |
| Surrounding settlements | dense settlement (urban area), light settlement (suburban area), rural area, industrial area |
| Vegetation | no vegetation, isolated vegetation, dense vegetation |
| Permitted air traffic | air traffic is permitted, air traffic is not permitted |
| Weather conditions | rainfall, snowfall, fog, cloudy, sunlight |
| Time of day | day, night |

be protected as it can exert influence on the detection capability of the drone. The states of this factor include the options of no vegetation around the asset, isolated vegetation or dense vegetation.

(18.) *Permitted air traffic*: describes whether or not air traffic is permitted in the area above and around the asset. States of this factor thus include on the one hand that air traffic is permitted and on the other hand that it is not permitted. This factor should be considered vigilantly due to the increasing number of regular drone flights, for example by parcelcopters, which can conduct parcel deliveries (Bamburry, 2015; Murray and Chu, 2015; Stolaroff et al., 2018).

(19.) *Weather conditions*: describes the weather condition that occur during the attack as it exerts influence on the detection capability (Müller, 2017). The weather conditions rainfall, snowfall, fog, cloudy and exclusive sunlight are listed as states.

(20.) *Time of day*: takes into account whether the attack takes place during the day or at night. These two possible conditions of this factor thus form the states, since the time of day also exerts an influence on the detection capability of a drone (Müller, 2017).

#### 3.1.1. *Results of the influence analysis*

A matrix consisting of all 20 factors was set up for the influence analysis, using a binary scale as described in Section 2.2. The directional influence assessment was conducted from the factor in row *i* to the factor in column *j*. Three experts ($n = 3$) in the field of drone and detection technologies were instructed to fill in the matrix. In order to combine the different assessments of the experts, the matrices were merged according to Eq. (1), whereby $x^v_{i,j}$ denotes the value entered of expert *v* in row *i* and column *j*.

$$x_{i,j} = \max\left\{x^1_{i,j}, x^2_{i,j}, ..., x^n_{i,j}\right\} \tag{1}$$

$$x^v_{i,j} = \{0, 1\} \tag{2}$$

For the analysis of the matrix, the active as well as the passive sums of the factors were calculated. Figure 2 shows a diagram in which the active sums are plotted against the passive sums of the factors. Factor six (*Intent*) shows the highest activ sum, while the passiv sum is the lowest. This factor thus represents the strongest system lever of the scenario space. Accordingly, a scenario is most strongly shaped by the intention of the attacker. Thus, clustering of scenarios based on different intentions is appropriate.

The remaining factors all show a high active sum as well as a high passive sum. Thus, they are all strongly involved in the system. The criterion for excluding a factor is met if it has either a low active sum or a low passiv sum. As no factor meets this criterion, all factors are used in further analysis as key factors.

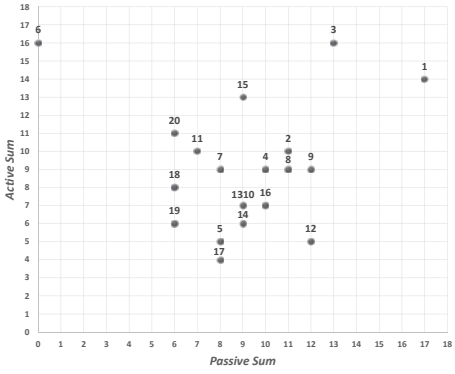


Fig. 2. Results of the Influence Analysis

#### 3.1.2. *Consistent scenarios*

Setting up the scenario space results in about two billion combinations of states. Herefrom, the consistent scenarios were identified based on the Cross-Impact Balance analysis. A five-point scale from −2 (total inconsistent) to +2 (strong directional support) was applied to evaluate the consistency of states in pairs. For this purpose, the 87 × 87 CIB-Matrix was set up to systematize the pairwise evaluation. Here, again, three experts ($n = 3$) were instructed to fill in the matrix independently. The matrices were merged according to Eq. (3). The mathematical evaluation of the CIB-Matrix was performed using the software *ScenarioWizard*.

$$y_{i,j} = \text{round}\left(\frac{y^1_{i,j} + y^2_{i,j} + ... + y^n_{i,j}}{n}\right) \tag{3}$$

$$y^v_{i,j} = \{-2, -1, 0, 1, 2\} \tag{4}$$

## 4. Derivation of Requirements

Based on the factor states of a scenario, requirements for a detection system can be derived. Some factor states of a scenario can be directly transferred into a requirement, whereas some requirements result from a combination of several factor states. A metric is necessary to systematically transfer the factor states into a list of requirements. This enables automated determination of

requirements from all scenarios. The approach used to derive requirements based on a scenario is described subsequently.

The first requirement for a detection system is the *range* at which the system must be able to detect a drone. The value for this requirement is composed of the factors *approach pattern, approach distance, intent, speed of the drone,* and *asset*. The required detection range $ra_x$ in scenario $x$ is derived by combining the speed of the attacking drone $s_x$, a value $p_x$ compensating the approach pattern and a reaction time $t_r$. The reaction time $t_r$ denotes the time necessesary to initiate countermeasures against the attack and depends on the intention of the attacker $I_x$ as well as on the asset $A_x$. The mathematical relation is described in Eq. (5). If the calculated range $ra_x$ is higher than the approach distance $r_x$, the requirement cannot be met due to the scenario properties (see Eq. (6)).

$$ra_x = p_x \cdot s_x \cdot t_r(I_x, A_x) \tag{5}$$

$$req_{\text{range}} = \begin{cases} ra_x \text{ if } ra_x \leq r_x \\ \text{✗} \quad \text{if } ra_x > r_x \end{cases} \tag{6}$$

The requirement for *weather resistance* describes whether the system should be able to provide robust detection in disruptive weather conditions. In certain scenarios, weather conditions complicate drone detection. Thus, detection system are required to resist such conditions depending on the scenario. For example, if snowfall is stated as the weather condition within the scenario, the system must be able to work under these conditions. The requirement concerning *object identification*, on the other hand, can be derived by considering the factors describing *surrounding settlements* and *permitted air traffic*. If the asset is located in an urban area or if air traffic is permitted on or around the asset, the detection system must be able to identify the approaching object to minimize false alarms. The factor *number of drones* can again be directly transferred into a requirement for the detection system. If the scenario describes the approach of a single drone, *multiple object detection* is not required. The same applies to the *detection in low light conditions*. This requirement is given when the scenario under consideration takes place at night or the weather condition is cloudy or rainy. Detection *independent of noise* is on the one hand required, if the drone in the scenario is operated with a silent propulsion system, such as a flapping wing drone. On the other hand, it is also necessary in a densely populated environment or in case of rainfall, where strong ambient noise prevails.

### 4.1. *Exemplary scenario based requirements derivation*

In this section, the requirements derivation is shown by using a consistent scenario resulting from the initial analysis. Table 2 lists the factor states of a randomly selected consistent scenario *e*. Table 3 summarizes the mentioned possible requirements, as well as their potential characteristics.

Table 2. Factor States of an exemplary scenario

| **Scenario (e)** |
|---|
| zig-zag path, 1 km, 0.2 km, no, is not used, espionage, 70 km/h, remote pilot controll, rotary wing, 0.2 km, 1 kg, no large contigous planes, no, single drone, research institute, light settlement, isolated vegetation, air traffic is not permitted, rainfall, day |

First, the required range $ra_e$ can be derived using Eq. (5) and Eq. (6). Therefore, the given quantities from scenario *e* should be noted. The speed of the drone in scenario *e* is $s_e = 70\,\text{km/h}$. Due to the zig-zag path of the drone, a compansating factor of $p_e = 0.6$ is assumed. In contrast, if the drone flies in a straight line towards the asset, a value of one would be assumed. The required reaction time is determined by the intention as well as the asset in scenario e. For an espionage attack on a research institution, a required response time of $t_r(I_e, A_e) = 60\,\text{s}$ is assumed. This value is based on expert interviews. Thus, the required range can be calculated according to Eq. (5). This results in a value of $ra_e = 0.7\,\text{km}$. Furthermore, the approach distance in this scenario ($r_e = 1\,\text{km}$) is higher than the required range (see Eq. (6)), which is why this requirement is feasible. Due to the occurrence of rainfall in the scenario, the detection system should be able to ensure detection even during rainfall. Object identification is not required in this scenario because air traffic is not permitted and the scenario takes place in a lightly settled area. Multiple object detection is not required, as a single approaching drone is described in the scenario.

Additionally, due to the rainfall, it is required that the detection system should provide detection in low light conditions and independent of noise. The derived requirements based on scenario *e* are listed in Table 3.

## 5. Conclusion and Outlook

A comprehensive scenario analysis was conducted to identify potential consistent threat scenarios

Table 3. Derivation of Requirements Based on a Scenario

| **Scenario** | **Requirements** | | | | | |
|---|---|---|---|---|---|---|
| | Range | Weather resistance | Object identification | Multiple object detection | Detection in low light conditions | Independent of noise |
| (x) | $ra_x$ | rainfall/ snowfall/ cloudy/ fog/ ✓ | ✓/ ✗ | ✓/ ✗ | ✓/ ✗ | ✓/ ✗ |
| (e) | 0.7 km | rainfall | ✗ | ✗ | ✓ | ✓ |

posed by civilian drones. The scenarios include information about the attacker's intent, tactics, capabilities, and the asset being threatened. In particular, factors that can be decisive for drone detection were addressed. The analysis includes critical infrastructures as attack targets since they are potentially of special interest for attackers. In summary, 20 factors and related states were identified based on literature review and expert interviews. Morphological analysis was used to set up the scenario space and Cross-Impact Balance analysis conducted to evaluate scenario consistency. By means of an influence analysis, the interrelationships of the factors in the system were analyzed and all factors were evaluated as key factors. Regarding the results, it can be highlighted that the intention of the attack exerts the strongest active influence on a scenario. Subsequently, the approach of a metric was presented to systematically translate the factor states of a scenario into requirements for a detection system. This enables a standardized evaluation of the consistent scenarios. In conclusion, this paper presents a comprehensive scenario analyis of threats posed by civilian drones including relevant parameters for drone detection. The results can be used to derive scenario-specific requirements for a detection system.

Within future work, further factors and states can be added to gain more detailed scenarios. This would enable elaborated requirements derivation serving as an information base to identify drone detection use cases.

## References


Altawy, R. and A. M. Youssef (2017). Security, privacy, and safety aspects of civilian drones. *ACM Transactions on Cyber-Physical Systems 1*(2), 1–25.

Alvarez, A. and T. Ritchey (2012). Outline for a morphology of modelling methods: Contribution to a general theory of modelling. *Acta Morphologica Generalis*.

Bamburry, D. (2015). Drones: Designed for product delivery. *Design Management Review 26*(1), 40–48.

BBK (2021). Sektoren und branchen kritischer infrastrukturen.

Bishop, P., A. Hines, and T. Collins (2007). The current state of scenario development: an overview of techniques. *Foresight 9*(1), 5–25.

Case, E. E., A. M. Zelnio, and B. D. Rigling (2008). Low-cost acoustic array for small uav detection and tracking. In *NAECON 2008 - IEEE National Aerospace and Electronics Conference*, Piscataway, NJ, pp. 110–113. IEEE.

Floreano, D. and R. J. Wood (2015). Science, technology and the future of small autonomous drones. *Nature 521*(7553), 460–466.

Garcia, M. L. (2017). Introduction to vulnerability assessment∗. In *Effective Physical Security*, pp. 23–53. Elsevier.

Gausemeier, J., A. Fink, and O. Schlake (1996). *Szenario-Management - Planen und Führen mit Szenarien* (Second ed.). Carl Hanser Verlag, München.

Gausemeier, J. and C. Plass (2014). *Zukunftsorientierte Unternehmensgestaltung: Strategien, Geschäftsprozesse und IT-Systeme für die Produktion von morgen* (2., überarb. Aufl. ed.). München: Hanser.

Guvenc, I., F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak (2018). Detection, tracking, and interdiction for amateur drones. *IEEE Communications Magazine 56*(4), 75–81.

Hassanalian, M. and A. Abdelkefi (2017). Classifications, applications, and design challenges of drones: A review. *Progress in Aerospace Sciences 91*, 99–131.

Johansen, I. (2018). Scenario modelling with morphological analysis. *Technological Forecasting and Social Change 126*, 116–125.

Müller, T. (2017). Robust drone detection for

day/night counter-uav with static vis and swir cameras.

Murray, C. C. and A. G. Chu (2015). The flying sidekick traveling salesman problem: Optimization of drone-assisted parcel delivery. *Transportation Research Part C: Emerging Technologies 54*, 86–109.

Ritchey, T. (2012). Outline for a morphology of modelling methods: Contribution to a general theory of modelling. *Acta Morphologica Generalis*.

Stolaroff, J. K., C. Samaras, E. R. O'Neill, A. Lubers, A. S. Mitchell, and D. Ceperley (2018). Energy use and life cycle greenhouse gas emissions of drones for commercial package delivery. *Nature Communications 9*(1), 409.

Taha, B. and A. Shoufan (2019). Machine learning-based drone detection and classification: State-of-the-art in research. *IEEE Access 7*, 138669–138682.

Valente, J. and A. A. Cardenas (2017). Understanding security threats in consumer drones through the lens of the discovery quadcopter family. *2017*, 31–36.

Vattapparamban, E., I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In *IWCMC 2016*, Piscataway, NJ, pp. 216–221. IEEE.

Weimer-Jehle, W. (2006). Cross-impact balances: A system-theoretical approach to cross-impact analysis. *Technological Forecasting and Social Change 73*(4), 334–361.

Wendt, P., A. Voltes-Dorta, and P. Suau-Sanchez (2020). Estimating the costs for the airport operator and airlines of a drone-related shutdown: an application to frankfurt international airport. *Journal of Transportation Security 13*(1-2), 93–116.