Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26247-cd

Threats based on civil airborne Drones: Developing and analyzing Scenarios for Ports

Sarra Majri

Department for Resilience of Maritime Systems, Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR). E-mail: sarra.majri@dlr.de

Frank Sill Torres

Department for Resilience of Maritime Systems, Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR). E-mail: Frank.Silltorres@dlr.de

Jan Stockbrügger

Department for Resilience of Maritime Systems, Institute for the Protection of Maritime Infrastructures, German Aerospace Center (DLR). E-mail: jan.stockbruegger@dlr.de

Ports play a central role in global trade and energy supply, making them critical nodes of modern infrastructure. Yet port operations are increasingly threatened by drones, causing major disruptions with potentially severe economic damages and consequences. This paper discusses the development and analysis of threat scenarios to study the impact of civilian drone misuse in ports. The derived scenario framework considers multiple parameters such as drone payload capacity, flight range, attack type and tactical conditions. These parameters are first defined and characterized and then combined into plausible threat scenarios. The methodological approach is based on a morphological box, which enables the systematic combination of parameter variations to form realistic and diverse attack scenarios. Subsequently, the generated scenarios are evaluated through a structured assessment process. The analysis identifies ports assets that represent particularly attractive targets from an attacker's perspective and derives correlations between drone capabilities, environmental conditions and asset vulnerability. The scenario mapping analysis shows the need for integrated drone countermeasures based on technical, operational and personal measures. Furthermore, the paper outlines potential countermeasures, including the evaluation of existing defense technologies and the development of criteria for safe and effective interception. The paper provides guidance for infrastructure operators to better protect their assets against civilian airborne drone attack, including non-technical defense approaches.

Keywords: Drones, Threat Scenarios, Ports, Critical Infrastructure, Vulnerability.

1. Introduction

Maritime infrastructures, such as ports and offshore wind farms, play a central role in global trade and energy supply chains. Disruptions or failures of maritime infrastructure can cause severe economic, environmental, safety and security consequences, including supply chain bottlenecks, vessel accidents, oil spills and broader threats to public safety. As a result, maritime infrastructures represent attractive targets for hybrid attacks and sabotage operations.

In this context, the increasing use of civilian airborne drones constitute a growing threat to port as critical nodes in global supply chain infrastructures. This is illustrated by past incidents in which alleged Russian drones have flown over strategically important ports in northern German and other relevant infrastructures highlighting the potential vulnerability of these infrastructures to espionage (Süddeutsche Zeitung 2026). Drones, probably launched from vessels, have also disrupted airport operations (Süddeutsche Zeitung 2025). Moreover, drone warfare in Ukraine has demonstrated that commercially available drones can be modified and converted into weapons systems with comparatively little effort (Chavez and Swed 2020).

Before proceeding, it is important to clarify the terminology used in this paper. The term drone is not limited to the flying object itself, but also includes the associated ground station and control system. In the literature, this is commonly referred to as an unmanned aerial vehicle or unmanned aircraft system (Chamola et al. 2020). For simplicity, the term "drone" will be used throughout this paper to refer to both the airborne vehicle and its control system.

Laws regulating the use of drone defense technologies vary across countries. In Germany, for instance, only the police can use counter drone technologies (Friedl and Rieckert 2020). A report by operators regarding overflights or similar would take too much time, meaning that it would no longer be possible to analyze the incident in detail. Consequently, there is a growing debate about allowing operators of critical infrastructures to use counter-drone systems to defend their assets.

Against this background, this paper aims to systematically develop and analyze threat scenarios for port infrastructures associated with civilian airborne drones. To do so the paper develops a morphological tool box of drone scenario parameters for ports that it then uses to construct specific threat scenarios. The toolbox can help analysts including port operators and security forces to identify realistic threat scenarios and plan countermeasures to protect assets.

This paper is structured in five sections. In the second section we provide an overview of relevant technical terms and introduce the methodological framework. Section three presents the derived threat scenarios. Section four handles the topic of a drone defense system. Finally, section five concludes the paper and outlines directions for future research.

2. Methodological framework

There are numerous methods available for scenario generation, varying in both the quantity and quality of scenarios produced. The selection of an appropriate method strongly depends on the defined research objective. A literature review identified morphological approaches as particularly suitable for developing and evaluating threat scenarios systematically, especially with regard to scenario consistency, transparency and integration (Kosow and Gaßner 2008, Ritchey 2002). Similar methodological approaches have also been applied in previous studies on security-related scenario analysis (Schneider et al. 2021).

2.1. Scenario Analysis with Cross-Impact-Balance

At the core of the methodological approach lies the concept of a morphological box. The morphological box is used to systematically structure the scenario space by identifying relevant parameters and their possible characteristics and by exploring their meaningful combinations (Ritchey 2002). In this way, the method helps to define the theoretical range of possible threat scenarios without making assumptions about their likelihood or internal consistency.

Building on this structured scenario space, Cross-Impact Balance analysis (CIB) is applied to assess how parameter characteristics interact and affect each other and to identify internally consistent scenarios. In this context, a scenario is considered consistent, when the selected descriptor characteristics support each other and do not create contradictory relationships.

CIB is a semi-qualitative method for developing scenarios based on the assumption that future developments result from the mutual influence of system factors. The first step of the approach is the definition of the system under investigation and the identification of relevant descriptors. Descriptors represent the key dimensions that characterize the scenario system. Based on literature research and expert input, several characteristics are defined for each descriptor, representing possible states within the scenario. Once the descriptors and their characteristics are defined, their combination forms the overall scenario space. The total scenario space is generated by combining all descriptor characteristics (Weimar-Jehle 2023).

The objective of CIB is to identify internally consistent scenarios by assessing how each characteristic influences the others using a predefined evaluation scale (see fig. 1). Positive values indicate a strengthening effect and negative values a weakening effect, and zero indicates no impact.

The morphological box is therefore transformed into a cross-impact matrix, allowing for a structured assessment of whether and to what extent one characteristic influences another characteristic (see fig. 1). Within the CIB framework,

only direct influences between characteristics are considered when assessing their interactions.

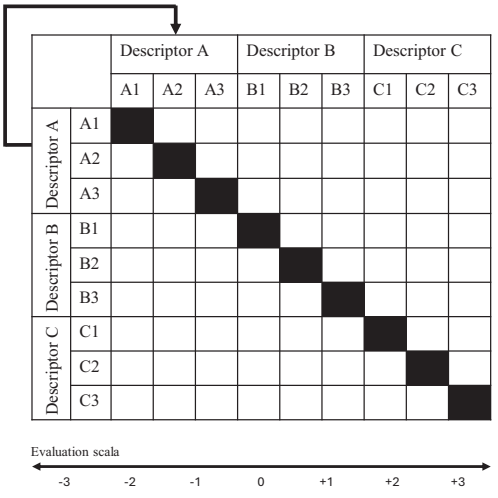

Figure 1: Layout CIB-Overview

Once all interactions are defined, the consistent scenarios can be calculated. For this, the four indicators impact sum, impact balance, consistency value and total impact score are relevant. Impact sum is defined by the sum of impacts of one characteristic (descriptor variant) while impact balance consists of all impact sums of a descriptor. The impacts are necessary for the consistency. The consistency value should be at minimum by zero. A scenario is considered consistent if its impact sum is at least as high as any alternative combination, meaning all its characteristics are mutually coherent and non-contradictory.

For further analyze the structure of the scenario system, active–passive diagrams can be used. This diagram visualizes how much each descriptor is influenced by others and the degree of influence they exert, providing insight into the dynamics of the scenario space (Weimar-Jehle 2023).

As the applied method is based on the combination of parameters and their characteristics, it is necessary to limit both the number of descriptors and their variations in order to manage complexity and ensure analytical clarity. An unrestricted expansion of descriptors would significantly increase the scenario space without necessarily improving the explanatory value of the analysis. Moreover, the definition of the descriptors and their relationships need to be clear and mutually exclusive (Weimar-Jehle 2023).

Therefore, a conscious reduction of parameters was applied. Based on literature research and expert discussions, the analysis was limited to a set of core descriptors that are considered important for describing drone-related threat scenarios associated with critical maritime infrastructures. These include the attacker profile, type of attack, attack environment, attack target and type of damage.

2.2. Experts as a Source of Information and Evaluation

As described in Section 2.1, expert knowledge represents an important source for identifying relevant descriptors and their characteristics as well as for assessing the relationships between them. The selection of experts followed the approach described by Bogner et al. (2014) and Niederberger and Wassermann (2015), who define experts as individuals possessing extensive professional knowledge and practical experience in a specific field.

Semi-structured expert interviews are suitable for collecting structured information. This interview format enables a systematic discussion of predefined topics and at the same time offers sufficient flexibility for the experts to contribute their specific perspectives and experiences. Interviews can be analyzed using qualitative content analysis.

3. Scenario Development

This section describes the application of the methodological framework introduced in Section 2. The objective here is to develop and analyze scenarios in which civil airborne drones may pose a threat to port infrastructures. Based on the principles of morphological analysis and CIB, relevant descriptors and their characteristics were identified, their interactions assessed and the resulting scenario space analyzed.

3.1 Identification of descriptors and characteristics

The descriptors and their characteristics were primarily identified through literature research and discussed and validated with experts. An overview is provided in table 1. In total, four experts

participated in the interviews. Their expertise covered areas related to drone technology and port infrastructure and to discuss potential relationships between these issues. For this purpose, a semi-structured interview guide was developed. The interview guide included thematic blocks addressing the definition of drone-related threats, the identification of relevant parameters for scenario generation and the discussion of possible relationships between these parameters

Table 1: Key literature used for the identification of descriptors and characteristics

Descriptors:	Authors:
Drone/ Attack/ Damage	Balashivudu, U., Jayanthi, S., Rani, M. S. and Shaheen, H. (2023)
	Chamola, V., Kotesh, P., Agarwal, A., Naren, Gupta, N. and Guizani, M. (2020)
	Hansen, P. and Faria, R. (2023)
	Publications Office of the European Union (2023)
	Chávez, K. and Swed, O. (2021)
Attackers	Chávez, K. & Swed, O. (2021)
Targets	Brinkmann, B. (2005)

Based on this process, the descriptors and their characteristics shown in table 2 were defined. Together, these descriptors capture the key dimensions of a drone-based threat scenarios.

Table 2: Descriptors and Characterizations for the CIB

Descriptor:	Characterization:
Drone profile	drone profile 1, drone profile 2, drone profile 3 & drone profile 4.
Attacker	individual attacker, extremist group, militant group & organized criminal networks.
Attack type	damage, smuggling, disruption & espionage.
Attack target	terminal, storage area, transport connection, dock gate, nautical facility, ship & building.
Environment	coast, waters, rural space, urban space & industrial space.
Damage type	property damage, environmental damage & public trust.

The sources are named in table 1.

The four drone profiles are distinguished by five operational characteristics (table 3). These characteristics were derived from publicly available data on commercially available drones between 2019 and 2023 (Oehler). For each parameter, minimum, maximum and average values were calculated in order to construct representative drone profiles.

Table 3: Characteristics of the four drone profiles

Characteristics:	DP 1	DP 2	DP 3	DP 4
payload [kg]	<0,1	<0,5	<1,0	<1,0
range [km]	<2	<4	<6	<6
flight time [min]	<20	<30	<40	<40
speed [km/h]	<35	<50	<70	<70
size [mm]	<213	<294	<520	<520

These five characteristics were identified as particularly relevant through literature research and discussions with experts from the respective infrastructure sectors. Although additional drone characteristics such as control systems or battery capacity could also be considered, the interviewed experts indicated that the selected parameters capture the most relevant operational capabilities and indirectly cover several other technical characteristics.

In addition to identifying the descriptors and their characteristics, the interactions between them were defined together with the experts. The resulting constellation of interactions between the descriptors is illustrated in Figure 2.

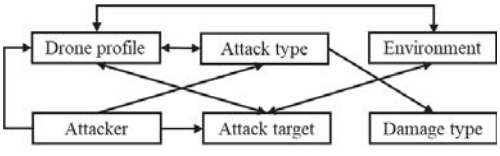

Figure 2: Interaction between the descriptors

Each expert assessed potential dependencies between descriptors. Based on these assessments, the relationships were evaluated using a predefined seven-point influence scale (table 4).

The scale captures both negative and positive influences between descriptor characteristics as well as neutral ones.

Table 4: Used evaluation scala

Influence effect:	Influence value:
Strong inhibiting influence	-3
Inhibiting influence	-2
Weak inhibiting influence	-1
No influence	0
Weak promoting influence	1
Promoting influence	2
Strong promoting influence	3

3.2 Scenario space generation and evaluation

Based on the defined descriptors and their characteristics, the overall scenario space was generated. Combining all characteristics resulted in 6,720 possible scenario combinations. The scenario generation and the identification of internally consistent scenarios were performed using the software ScenarioWizard.

Applying the analysis reduced the initial scenario space to 213 internally consistent scenarios. The total impact score is between 32 to 36 and the consistency value is by zero. The strength and direction of the interactions between descriptors directly influence the consistency of the generated scenarios. For further analyze these relationships, an active/passive diagram was used (fig. 3). In this context, active descriptors refer to those exerting influence on other descriptors, whereas passive descriptors are primarily influenced by others.

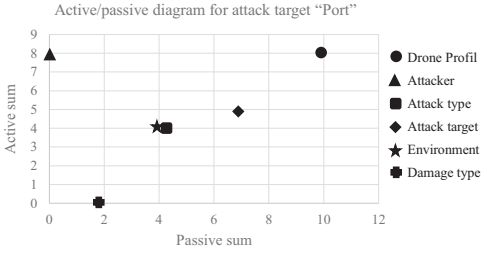

Figure 3: Active/Passive-Diagram

The diagram provides an overview of the quality and strength of interactions between the descriptors. The active and passive sums are derived by aggregating the influence values assigned to each characteristic, where active values represent the influence exerted on other descriptors and passive values represent the influence received. The evaluation scale used for this purpose is based on expert interviews and supported by the literature.

To illustrate the interpretation of the diagram, the descriptor damage type can be used as an example. The type of damage largely depends on the type of attack; once the attack type is known, the resulting damage becomes more predictable (see fig. 2). This dependency is visible in figure 2. At the same time, the attack type itself is influenced by the drone profile, indicating an indirect indirect linkage that is implicitly considered through the network of direct influences in the CIB analysis.

With regard to the objective of identifying vulnerable assets, the descriptor attack target is characterized by a high passive value, meaning that it is influenced by multiple other descriptors. One reason for this is that attackers typically decide first what they intend to attack. At the same time, the attack target also exhibits a high active value, as it influences the selection of other scenario characteristics, such as the attack type and the resulting damage. Although the characteristics of a target may also shape attacker behavior, the direction of causality is ambiguous and difficult to determine. Nevertheless, once the target is defined, the structure of a plausible scenario becomes significantly clearer.

Overall, most descriptors exert direct or indirect influence on the attack target. This indicates that a comprehensive understanding of these interactions is important for improving the protection of critical assets.

3.3 Analysis of consistent scenarios

Focusing on the consistent scenarios based on the attack target, the analysis concentrates on scenarios in which the drone profile, attack target and attack type are central, as these descriptors exhibit the strongest interactions and highest impact values within the CIB analysis. A closer examination shows that multiple damage types may result from a single attack. Within the analysis, these damage types are initially treated as separate characteristics. For the purpose of scenario reduction and improved interpretability, they are aggregated, allowing multiple damage types to be assigned to a single scenario. Based on this approach, 213 individual cases were summarizing into 93 scenarios. Table 5 gives an overview of the consistent scenarios sorted by the attack targets.

Table 5: Number of scenarios sorted by attack target

Attack target:	Sum of Scenarios:
Terminal	6
Nautical facility	8
Storage area	11
Ship	12
Transport connection	14
Dock gate	19
Building	23

This distribution indicates that transport connection, dock gates and buildings occur most frequently as potential attack targets and can therefore be considered particularly vulnerable assets within the analyzed scenario space. From these three targets, just building is represented in all of the four total impact scores.

That means, that buildings mainly are attractive targets and so vulnerable. A comparison with other descriptors shows that all drone profiles appear in scenarios involving these targets, indicating that a wide range of drone capabilities could potentially be used in such attacks.

Regarding the attack types, damage and disruption dominate the scenario space, occurring 43 and 34 times respectively. This suggests that direct attacks and operational disruptions represent the most plausible forms of drone-related threats in the analyzed context. Damage is therefore characterized as a strongly passive descriptor, as it is influenced by the combination of all other descriptors. This observation corresponds with the interaction patterns identified in the analysis.

Overall, the results indicate that several combinations of drone capabilities, attacker profiles and attack types may lead to scenarios in which transport connection, dock gate and buildings represent particularly vulnerable targets. However, it should be emphasized that the results are derived from a semi-qualitative scenario analysis. Consequently, the results may vary depending on the applied evaluation scale, the selection of descriptors or the expert assessments used in the analysis.

4. Drone defense for ports

From a functional perspective, drone defense system can be described as a sequence of interdependent phases. The four distinct phases are detection, identification, tracking and neutralization. However, these technical phases cannot be considered in isolation. They must be connected to operational and personal measures (see fig. 4) in order to build an effective and resilient drone defense system. Consequently, it should be understood as a socio-technical system rather than a technical solution.

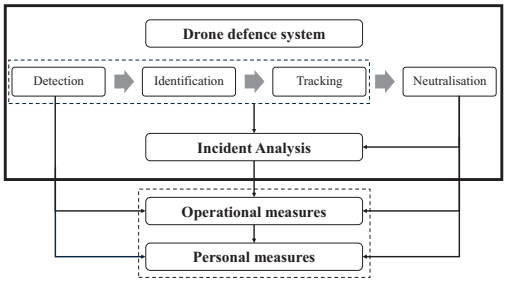

Figure 4: Process of defense based on Hansen and Faria 2023

This figure illustrates the functional process of drone defense and its interaction with operational and personal measures. The figure highlights that effective protection is achieved only when technical systems, organizational structures and human decision-making are aligned.

Within this system, detection represents the initial and most critical phase, as all subsequent actions depend on the timely recognition of a potential threat. Various technical approaches can be applied for drone detection, including radar systems, radio-frequency sensors, acoustic sensors and optical systems. Each of these technologies exhibits specific strengths and limitations that must be carefully evaluated in relation to the port environment.

Radar-based detection systems, for instance, are capable of detecting small airborne objects over open water and at relatively long distances, even under adverse weather conditions. However, in complex port environments their performance may be reduced due to reflections from cranes, vessels and buildings, as well as difficulties in distinguishing drones from birds or other moving objects. Radio-frequency-based detection systems, by contrast, are particularly effective in identifying manually operated drones by detecting communication links between the drone and its remote controller. Yet, this method is largely ineffectiveness against fully autonomous drones or in environments with high levels of electromagnetic

interference, which are common in ports due to nautical and industrial infrastructure. These limitations demonstrate that no single detection technology is sufficient on its own, emphasizing the need for multi-sensor approaches, sensor fusion and site-specific adaptation (Yaacoub et al. 2020).

Neutralization techniques can generally be divided into passive and active measures. Passive measures include jamming, spoofing or cyber-based interventions, which aim to disrupt navigation or communication systems. Active measures, such as nets, projectiles, high-energy lasers or high-power microwaves, physically interfere with or destroy the drone. Both approaches involve distinct advantages and risks. Passive measures allow the controlled landing and subsequent forensic analysis of a drone, supporting incident investigation and learning processes. Active measures, on the other hand, are often better at eliminating a threat, but they can introduce secondary risks, particularly in densely built port areas or if hazardous payloads are involved. It might be necessary to designate a safe landing zone if the drone carries explosives. These considerations underline the need for predefined safe zones for interception or landing, exclusion areas for personnel and clear decision thresholds to avoid harm to people, infrastructure or port operations (Chamola et al. 2021).

Beyond the technical dimension, operational and personal measures play an important role throughout all phases of the drone defense process. Operators must possess detailed knowledge of the port layout, critical assets and environmental conditions. Clear organizational structures, defined responsibilities and established communication channels with emergency and security authorities are important to ensure coordinated responses. Regular training and exercises are necessary to enable personnel to correctly interpret system outputs and act effectively under time pressure.

Figure 4 further illustrates that a drone defense system does not end with the neutralization attempt itself. Depending on whether the defense is successful or not, post-incident analysis can provide valuable insights into attack patterns, system performance and response effectiveness. This feedback loop contributes to the continuous improvement of counter-drone measures and supports the long-term reduction of vulnerabilities in critical maritime infrastructures.

5. Conclusion and Outlook

This paper examined the vulnerability of critical maritime port infrastructures to drone-based threats by applying a scenario-mapping approach. The results demonstrate that even commercially available drones with limited technical capabilities can pose significant risks to high-value assets. These findings underline the increasing relevance of drone threats for ports and the urgent need for structured and integrated protection concepts.

By mapping vulnerabilities across different attack scenarios, the analysis highlights that effective counter-drone defense cannot be achieved through isolated technical solutions alone. Instead, drone defense must be understood as a socio-technical system that integrates technical capabilities with operational planning and trained personnel. The functional phases of detection, identification, tracking and neutralization are highly interdependent and weaknesses in any single phase may substantially reduce the effectiveness of the overall system.

The evaluation of existing counter-drone technologies shows that each technical approach entails specific strengths and limitations that are strongly influenced by the complex and dynamic characteristics of port environments. Consequently, the selection and deployment of counter-drone measures must be site-specific and based on a detailed understanding of local infrastructure, operational processes and environmental conditions. In this context, the analysis emphasizes the importance of combining active and passive neutralization measures with clearly defined operational procedures, safe zones and decision criteria to ensure both effectiveness and safety.

Beyond technical measures, organizational preparedness and personnel competence emerge as critical factors for reducing vulnerability. Clear roles, responsibilities and communication structures, as well as regular training and exercises, are essential to enable timely and coordinated responses under the limited reaction times associated with drone attacks. Post-incident analysis further represents a valuable mechanism for learning and continuous improvement, supporting

the adaptation of counter-drone concepts to evolving threat patterns.

Looking ahead, future research should increasingly focus on emerging drone technologies and their implications for critical maritime infrastructures. In particular, drone swarming technology represents a significant challenge for existing counter-drone systems. Swarms can overwhelm detection and neutralization capabilities, exploit system saturation effects and reduce the effectiveness of single-target interception strategies. Addressing such threats will require advances in multi-sensor fusion, automated decision support and coordinated neutralization concepts capable of responding to multiple simultaneous targets.

Further research should also explore the integration of counter-drone systems into broader port security and resilience frameworks, traffic management and emergency response planning. Developing standardized evaluation criteria and best-practice guidelines may support infrastructure operators in selecting and implementing effective counter-drone measures.

In conclusion, this paper demonstrates that reducing the vulnerability of ports to drone threats requires an integrated, scenario-based approach that combines technical, operational and personnel measures. As drone technologies continue to evolve, adaptive and resilient counter-drone concepts will be essential to ensure the long-term security and functionality of critical maritime infrastructures.

References

Brinkmann, Birgitt. *Seehäfen*. Berlin, Germany: Springer, 2004. https://doi.org/10.1007/b138397.

Bogner, Alexander, Beate Littig, and Wolfgang Menz. *Interviews mit Experten: Eine praxisorientierte Einführung*. Wiesbaden:. Springer VS, 2014. https://doi.org/10.1007/978-3-531-19416-5.

Chamola, Vinay, Pavan Kotesh, Aayush Agarwal, Naren, Navneet Gupta, and Mohsen Guizani. "A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques". *Ad Hoc Networks* 111 (2021): 102324. https://doi.org/10.1016/j.adhoc.2020.102324.

Chávez, Kerry, and Ori Swed. "The Proliferation of Drones to Violent Nonstate Actors". *Defence Studies* 21, no. 1 (2 January 2021): 1–24. https://doi.org/10.1080/14702436.2020.1848426

Deutsche Presse-Agentur (dpa). 2025. "Drohnen in Dänemark – Festnahme auf verdächtigem Schiff." *Süddeutsche Zeitung*, October 1, 2026. https://www.sueddeutsche.de/wirtschaft/drohnen-alarm-drohnen-in-daenemark-festnahmen-auf-verdaechtigem-schiff-dpa.urn-newsml-dpa-com-20090101-251001-930-112524.

Deutsche Presse-Agentur (dpa). 2026. "Immer öfter Drohnen über Militäreinrichtungen und Häfen." *Süddeutsche Zeitung*, January 1, 2026 https://www.sueddeutsche.de/politik/sicherheit-im-norden-immer-oefter-drohnen-ueber-militaer-einrichtungen-und-haefen-dpa.urn-newsml-dpa-com-20090101-260101-930-485525.

Friedl, A., and U. Rieckert. "Neue Gefährdungslagen: Detektion und Abwehr gefährlicher Drohnen durch die Polizei". Deutsches Polizeiblatt für Aus- und Fortbildung 6 (2020): S. 25- 30.

Hansen, P., and R. Pinto Faria. "Protection against unmanned aircraft systems". Publications Office of the EU. Publications Office of the European Union, 2023. https://doi.org/10.2760/18569.

Kosow, Hannah, and Robert Gaßner. *Methoden der Zukunfts- und Szenarienanalyse: Überblick, Bewertung und Auswahlkriterien.* Berlin: Institut für Zukunftsstudien und Technologiebewertung, 2008.

Niederberger, Marlen, and Sandra Wassermann, eds. *B. Methoden der Experten- und Stakeholdereinbindung in der sozialwissenschaftlichen Forschung.* Wiesbaden, Germany: Springer Fachmedien, 2014. https://doi.org/10.1007/978-3-658-01687-6.

Oehler, Jens. n.d. "Drohnen-Statistiken pro Jahr." *Drohnen.de.* Accessed November 20, 2024. https://www.drohnen.de/38904/drohnen-statistik/

Publications Office of the European Union. "Protection against Unmanned Aircraft Systems". Publications Office of the EU. Publications Office of the European Union, 18 October 2023. https://doi.org/10.2760/969680.

Schneider, Moritz, Daniel Lichte, Dustin Witte, Stephan Gimbel, and Eva Brucherseifer. "Scenario Analysis of Threats Posed to Critical Infrastructures by Civilian Drones". In *Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021)*. Singapore: Research Publishing Services, 2021. https://doi.org/10.3850/978-981-18-2016-8_234-cd.

Weimer-Jehle, Wolfgang. *Einführung in die Cross-Impact-Bilanzanalyse (CIB): Wege zur qualitativen System- und Szenarioanalyse.* Wiesbaden: Springer Gabler, 2023.

Yaacoub, Jean-Paul, Hassan Noura, Ola Salman, and Ali Chehab. "Security Analysis of Drone Systems: Attacks, Limitations, and Recommendations." *Internet of Things* 11 (2020): 100218. https://doi.org/10.1016/j.iot.2020.100218