Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Technology Readiness and Airport Security: Crisis Management of Drone Threats at Kuala Lumpur International Airport

Helal Ahmed Saif Abdulla Albooshi[1], Haryati Binti Shafii[2]
[1,2]Faculty of Technology Management and Business, Universiti Tun Hussein Onn Malaysia
Johor Darul Ta'zim, Malaysia

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Introduction: Drone incursions pose increasing risks to aviation security, requiring airports to strengthen technological and organizational preparedness.

Objectives: This study examines how technology readiness and technology usage influence crisis management effectiveness at Kuala Lumpur International Airport (KLIA).

Methods: Employing a quantitative design, data were collected from 136 management and security-related staff, with SPSS used for descriptive analysis and SmartPLS for assessing the measurement and structural models.

Results: The findings show that three dimensions of technology readiness technology adoption, infrastructure preparedness, and staff training significantly enhance crisis management, mainly through their impact on technology usage. Policy and procedures, while necessary for governance, showed no significant direct influence on technology usage or crisis response. Technology usage itself demonstrated a strong positive effect on crisis management and served as a key mediating factor linking readiness components to crisis outcomes.

Conclusions: Based on these results, the study proposes a structured framework emphasizing advanced technology integration, resilient infrastructure, continuous training, and alignment of policies with operational practices. The study contributes theoretically by clarifying the mechanisms through which readiness drives crisis effectiveness, and practically by offering a model for improving drone threat management in aviation settings. The findings provide actionable insights for airport authorities and regulators working to enhance preparedness against emerging unmanned aerial system (UAS) threats.

Keywords: technology readiness, technology usage, crisis management, drone threats, aviation security, KLIA.

INTRODUCTION

The rapid advancement of Uncrewed Aerial Systems (UAS) has transformed multiple industries but has also introduced significant security risks to the aviation sector. Due to their affordability, accessibility, and operational flexibility, drones have increasingly appeared in restricted airport airspace, threatening passenger safety, flight operations, and airport security. Global incidents including the Gatwick and Frankfurt airport shutdowns, which resulted in over 800 cancelled flights and more than 120,000 stranded passengers demonstrate the severity of drone-related disruptions (News, 2018). Drone misuse has extended beyond operational interference to malicious activities, such as the 2019 attack on a Saudi oil facility (Dudenhoeffer, 2020) and the 2018 attack on a Russian military base (Samaan, 2020). These events highlight the escalating challenge airports face in mitigating drone incursions.

Traditional airport security measures, such as perimeter fencing and visual surveillance, are inadequate against small, fast-moving drones that can evade detection, especially at night. Moreover, conventional countermeasures are limited because they may endanger aircraft or violate regulatory restrictions. This gap highlights the need for advanced technological solutions, including automated detection systems, geofencing, and integrated counter-drone technologies (Balci, 2023). However, implementing such technologies requires careful integration with existing security frameworks, adherence to evolving regulatory requirements, and trained personnel capable of operating these systems effectively.

Crisis management plays a crucial role in maintaining organizational resilience in such high-risk environments. Crises whether natural or man-made remain unpredictable and require timely and coordinated responses (Pedersen et al., 2020; Sandin, 2018). In the aviation sector, the increasing complexity of technology has heightened both the opportunities and vulnerabilities associated with crisis response (Raspotnig et al., 2020). Airports have benefited from technological innovations, including surveillance tools and automated safety systems, yet these advancements have also exposed new ethical and operational challenges (Al Shobaki et al., 2016; Amuna et al., 2017).

As drone usage continues to grow globally, with the market projected to reach USD 163.60 billion by 2030 (Grand View Research, 2025), the potential for misuse intensifies. Drones can interfere with airport communications, conduct unauthorized surveillance, and cause mid-air collisions (Hern & Topham, 2018). Strategies such as GPS-based detection and geofencing have been explored to mitigate such risks, but airports require comprehensive, technology-driven crisis management frameworks to ensure operational continuity and safety (Bennett, 2019; Weaver et al., 2018).

Given these global challenges, Kuala Lumpur International Airport (KLIA) faces a pressing need to strengthen its crisis management capabilities through appropriate technology adoption. KLIA's operational environment, traffic volume, and national security considerations require tailored technological solutions that go beyond standard international templates. Assessing the airport's readiness spanning infrastructure, staff training, technology usage, and policy implementation is essential for developing an effective drone threat management framework. This research therefore investigates KLIA's technological preparedness and proposes an evidence-based framework to improve crisis response, enhance aviation safety, and protect passengers, crew, and airport operations.

RESEARCH OBJECTIVES

The primary objective of this study is to assess the readiness level of technological adoption for managing drone-related crises at Kuala Lumpur International Airport (KLIA) in Malaysia. To achieve this goal, the study aims to evaluate key factors influencing technology readiness and its impact on crisis management effectiveness. Based on this objective, the following specific research objectives have been formulated:

1. To examine the impact of technology readiness factors (staff training, technology adoption, infrastructure preparedness, and policy & procedures) on the crisis management of drone threats at KLIA.
2. To investigate the mediating role of technology usage in the relationship between technology readiness and the crisis management of drone threats at KLIA.

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

Overview of Drone Technology Adoption and Issues at Airports

Unmanned Aerial Vehicles (UAVs), or drones, offer valuable applications for monitoring, surveillance, and operational support in aviation environments (Saad et al., 2020). Their increasing affordability and public acceptance have expanded their use across sectors, including airport security (Sandbrook, 2015; Wright, 2014). Although drones may provide operational benefits and even support potential commercial transport services (Price & Forrest, 2016; Sammler & Lynch, 2021), they present significant safety and security risks. Many drone-related challenges arise from operators who lack awareness of aviation rules or intentionally violate them, resulting in unauthorized flights near restricted airport zones (Calandrillo et al., 2020; Price & Forrest, 2016).

Drones can be weaponized, used for illegal activities, or cause runway closures, collisions, and near misses, threatening both operational continuity and passenger safety (Pyrgies, 2019). The European Union Aviation Safety Agency (EASA, 2021) highlights varying risk levels across different categories of drone operations, including unauthorized flights near critical airport infrastructure. These risks place additional pressure on airport authorities to manage legal, policy, and cybersecurity issues related to drone incursions (Balci, 2023; Reitz, 2025).

Overview of Crisis Management

A crisis is any unexpected event that disrupts normal operations and threatens organizational stability, reputation, or safety (Waryjas, 1999). Crises may arise from natural disasters, technological failures, or deliberate acts such as drone attacks or terrorism (Bolt et al., 2013; Keller et al., 2016). Effective crisis management involves rapid response, communication, and coordinated strategies to minimize harm (Pedersen et al., 2020). Technology increasingly shapes crisis management capabilities, enabling better detection, communication, and decision-making (Raspotnig et al., 2020). In aviation, technological tools have exposed unethical practices, improved safety, and reduced operational risks (Dias, 2024). Emerging technologies such as drone detection systems and signal monitoring further support crisis response (Sciancalepore et al., 2019).

Underpinning Theory

This study uses both the Situational Crisis Communication Theory (SCCT) and the Technology-Organization-Environment (TOE) framework, which together offer a comprehensive lens for understanding technology-based crisis management at KLIA.

SCCT, developed by Coombs (2007), explains how organizations protect their reputation during crises by aligning response strategies with stakeholders' attributions of responsibility. When stakeholders perceive that a crisis could have been prevented or that the organization bears high responsibility, they expect more accommodative responses, such as apology and corrective action (Dulaney & Gunn, 2017). Previous crises and poor prior relationships intensify reputational risk, requiring more transparent and responsible communication (Brown et al., 2016). In the context of drone threats, SCCT helps frame how KLIA's preparedness and response supported by technology shape stakeholder perceptions of competence and responsibility.

The TOE framework explains technology adoption through three contextual dimensions: technological, organizational, and environmental. The technological context involves the availability, benefits, and compatibility of technologies such as drone detection and crisis monitoring systems (Baker, 2012). The organizational context includes internal readiness factors such as staff capabilities, infrastructure, and policies (Oliveira & Martins, 2011). The environmental context reflects external pressures such as regulations, security threats, and industry standards (Zhu et al., 2006). In this study, technology readiness (staff training, technology adoption, infrastructure, policies) is located within the technological and organizational domains, while the broader drone-threat environment forms the external driver for readiness and adoption (Hauberg, 2011). SCCT clarifies the strategic communication dimension of crisis response, while TOE explains the internal conditions enabling KLIA to adopt and use technologies that support that response.

Conceptual Framework and Research Hypothesis

This study proposes a conceptual framework for managing drone-related crises at KLIA. Crisis management effectiveness, defined as how well the airport prepares for and responds to drone threats, is the dependent variable. Technology readiness is the independent variable, comprising four dimensions: staff training, technology adoption, infrastructure preparedness, and policy and procedures. Technology usage is modelled as a mediating variable that links readiness to crisis management by capturing the extent to which available technologies are actually utilized during prevention, detection, and response activities as illustrated in Figure 1.

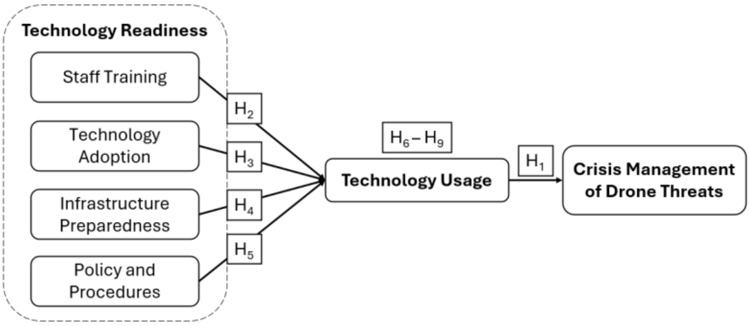


Figure 1. Conceptual Framework

The framework assumes that higher levels of technology readiness enhance technology usage, which in turn improves crisis management performance. It therefore focuses on the combined effects of human capability, technological tools, infrastructure, and formal procedures on KLIA's resilience to drone threats.

Technology Readiness

The growing use of drones around airports demands a comprehensive readiness strategy that integrates human, technical, and procedural capacities. In this study, technology readiness consists of four interrelated components, which are as follow.

Staff Training

Staff training is the first line of defence against drone threats. Well-trained personnel are better able to identify suspicious drone activity, follow emergency protocols, and operate counter-drone systems. Regular, structured training enhances situational awareness and accuracy of response (ICAO, 2025). Simulation-based exercises and scenario drills, including the use of tools such as augmented reality and crisis simulations, can strengthen preparedness for real-time incidents (Department of Homeland Security, 2023).

Technology Adoption

Technology adoption refers to the deployment of advanced systems for detecting, tracking, and neutralizing unauthorized drones. These include radar, radio-frequency sensors, geo-fencing, artificial intelligence-based surveillance, and integrated command platforms. Such systems enable proactive monitoring of restricted airspace and provide data for timely decision-making (Testoni et al., 2021). Effective adoption also involves using digital platforms for logging incidents, sharing information, and analysing past events to refine response strategies.

Infrastructure Preparedness

Infrastructure preparedness covers the physical and digital systems that support crisis response. This includes secure operational zones, sensor networks, control rooms, and communication channels linking security units, air traffic control, and management teams. Airports with clearly defined response zones, drone detection perimeters, and emergency control points experience fewer and shorter disruptions (EASA, 2021). Robust and redundant communication infrastructure is essential to coordinate actions under time pressure.

Policy and Procedures

Policies and procedures provide formal guidance for handling drone threats. They define roles, responsibilities, reporting lines, and criteria for escalation, as well as rules for activating counter-drone measures and engaging external agencies such as law enforcement. Effective policy frameworks are developed collaboratively with regulators, operators, and technology providers and are regularly updated to reflect new threat patterns and regulatory changes (National Academies of Sciences, 2025). In combination, these four dimensions reflect the overall technology readiness of an airport like KLIA. Their interaction determines the organization's ability to prevent, detect, and respond to drone-related crises in a consistent and coordinated manner.

Technology Usage

Technology usage refers to the actual, routine use of available technological tools in crisis management rather than their mere presence. Advances in information and communication technologies have expanded the channels through which organizations can detect threats, communicate with stakeholders, and coordinate responses (Alam et al., 2018; Saroj & Pal, 2020).

In crisis situations, technology supports functions such as early warning, real-time monitoring, decision support, and post-incident analysis (Schröter et al., 2020). Social media and digital platforms also provide valuable, time-sensitive information from eyewitnesses and the public, which crisis teams can monitor and verify to improve situational awareness (Amaral, 2019; Plotnick & Hiltz, 2018).

However, there is no single, ideal technological solution for crisis communication and coordination. Organizations differ in their resources, stakeholder needs, and regulatory environments, which affects how technologies are selected and used (Cook et al., 2019; White, 2011). Prior research shows that many stakeholders recognize the potential of crisis technologies but do not fully utilize them, often due to usability issues, limited awareness, or access barriers (Comes et al., 2019; Zhang et al., 2020). In this study, technology usage captures how far KLIA integrates and operationalizes its technological tools such as surveillance systems, communication platforms, and incident management systems in responding to drone threats.

Crisis Management

Crisis management is the process of anticipating, preparing for, responding to, and recovering from events that threaten an organization's operations, reputation, or stakeholders (Parker et al., 2020; Ritchie & Jiang, 2019). Effective crisis management depends on early detection, clear situational awareness, and structured plans that guide actions under pressure (Varma, 2019).

In the aviation context, crises may arise from security breaches, technological failures, natural hazards, or emerging threats such as unauthorized drones (McCaffrey et al., 2020). High-reliability organizations emphasize strong communication, teamwork, and continuous monitoring to avoid catastrophic failures in such complex environments (Bongiovanni & Newton, 2019).

Crisis management teams therefore require specialized skills, clear roles, and reliable information to coordinate responses across multiple agencies and stakeholders (Tagarev & Ratchev, 2020). At an international airport, crisis management planning must also consider wider social responsibilities such as supporting emergency relief, handling stranded passengers, and maintaining essential operations during large-scale disruptions (Mijović et al., 2019). In this research, crisis management effectiveness represents KLIA's ability to manage drone-related incidents in a timely, coordinated, and safe manner, minimizing disruption to operations and risk to passengers and staff. The specific statements outlining these hypothesized relationships are provided as follows.

Direct effects

H1: Technology usage has a significant positive effect on the crisis management of drone threats at KLIA.

H2: Staff training has a significant positive effect on technology usage for managing drone threats at KLIA.

H3: Technology adoption has a significant positive effect on technology usage for managing drone threats at KLIA.

H4: Infrastructure preparedness has a significant positive effect on technology usage for managing drone threats at KLIA.

H5: Policy and procedures have a significant positive effect on technology usage for managing drone threats at KLIA.

Mediating effects

H6: Technology usage significantly mediates the relationship between staff training and the crisis management of drone threats at KLIA.

H7: Technology usage significantly mediates the relationship between technology adoption and the crisis management of drone threats at KLIA.

H8: Technology usage significantly mediates the relationship between infrastructure preparedness and the crisis management of drone threats at KLIA.

H9: Technology usage significantly mediates the relationship between policy and procedures and the crisis management of drone threats at KLIA.

MATERIALS AND METHODS

The study adopted a quantitative research design as a systematic strategy for selecting participants, research sites, and data collection methods to address the research questions. Research design functions as the structural link between the research problem and the implementation of appropriate methods (Hauberg, 2011), guiding instrument development, fieldwork, data collection, and analysis (Azizan & Lim, 2023). A descriptive and quantitative approach was selected to measure key variables, using numerical data that allow for statistical testing, prediction, and generalization (Matović & Ovesni, 2023; Rahi, 2017). This choice aligns with the study's aim to examine correlations and test causal relationships across a large population, consistent with the principles of objective, systematic measurement (McLeod & Curtis, 2020).

Research Population and Sampling

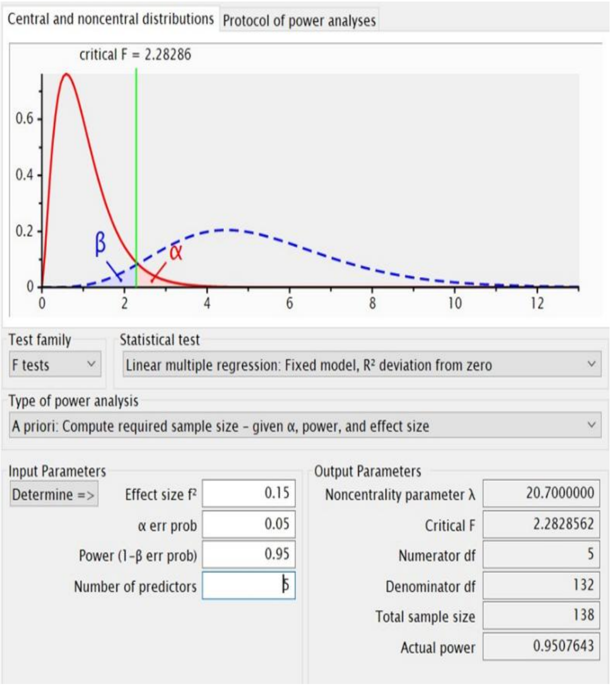
The research population refers to all individuals who share the characteristics relevant to the study (Ritchie & Jiang, 2019), and in the context of KLIA this includes the 426-management staff responsible for security and crisis management, drawn from a total workforce of 9,459 employees as reported in the Malaysia Airports Holdings Berhad Sustainability Report 2019. These personnel constitute the target population because they are directly involved in responding to drone-related threats and are best positioned to provide accurate insights.

Table 1. Research Population

Employees	Permanent		Contract		Total
	Female	Male	Female	Male	
Senior Management	–	–	2	7	9
Management	125	265	9	27	426
Executive	398	657	–	4	1,055
Non-executive	2,623	5,132	110	100	7,965
Total	**3,146**	**6,054**	**121**	**138**	**9,459**

Source: Malaysia Airports Holdings Berhad Sustainability Report 2019

A research sample is a manageable subset of this population (Kothari, 2004), and in this study, management staff were selected because of their critical operational roles. To determine an appropriate sample size, the study used G*Power, which offers flexible statistical estimation based on effect size and desired power (Erdfelder et al., 2009).


Central and noncentral distributions
Protocol of power analyses
critical F = 2.28286
0.6
0.4
0.2
0
0
2
4
6
8
10
12
β
α
Determine =>

Test family: F tests
Statistical test: Linear multiple regression: Fixed model, R² deviation from zero
Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters
Effect size f²: 0.15
α err prob: 0.05
Power (1-β err prob): 0.95
Number of predictors: 5

Output Parameters
Noncentrality parameter λ: 20.7000000
Critical F: 2.2828562
Numerator df: 5
Denominator df: 132
Total sample size: 138
Actual power: 0.9507643

Figure 2. Power analysis output for sample size estimation

The analysis recommended a minimum of 138 respondents, which the study achieved as illustrated in Figure 2. Given operational constraints and limited access to all staff, a convenience sampling technique was used, with questionnaires distributed digitally via QR code to the respondents. This approach ensured accessibility, voluntary participation, and feasibility while maintaining alignment with the study's objectives and the statistical requirements for reliable analysis.

Data Collection Instrument

A structured questionnaire was used as the primary data collection instrument, because the research objectives required obtaining direct perceptions from KLIA personnel rather than relying on publicly available data. Questionnaires are suitable for collecting large amounts of confidential and cost-effective data within a short timeframe (Regmi et al., 2016). The questionnaire design followed established guidelines emphasizing clarity, relevance, and concise wording to avoid ambiguity. Measurement items were adapted from validated empirical studies and also undergo a pilot study to strengthen reliability (Arafat et al., 2016). A five-point Likert scale ("1 = Strongly Disagree" to "5 = Strongly Agree") was used for all items, as it allows consistent classification of responses and facilitates statistical analysis. Completed questionnaires were screened for missing data and response bias before being processed for analysis, ensuring validity and reducing common method error.

Data Analysis

The two-stage data analysis approach using IBM SPSS and SmartPLS was used in the study. SPSS was first used for data cleaning, screening, and descriptive analysis, including checks for missing values, outliers, normality, and demographic profiling through frequencies and percentages. Descriptive statistics such as mean, standard deviation, minimum, and maximum scores provided an overview of respondent perceptions, following established interpretation scales (Alkharusi, 2022). After confirming data reliability, Partial Least Squares Structural Equation Modelling (PLS-SEM) using SmartPLS was applied to evaluate both the measurement model assessing reliability and validity and the structural model, which was used to test the study's hypotheses. PLS-SEM is appropriate for analysing latent constructs and complex relationships, making it suitable for this research context. Consistent with Bougie and Sekaran (2019) and Miles (1994) guidelines, the analysis process involved iterative stages of data reduction, data display, and conclusion drawing, ensuring systematic interpretation and robust findings. This integrated analytical approach strengthened the study's ability to evaluate technology readiness, technology usage, and crisis management relationships effectively.

RESULTS

Demographic Results

The sample consisted of 136 respondents as presented in Table 2, with a majority being male (63.2%), which reflects the gender distribution commonly found in aviation operational and security-related roles. The age structure shows a relatively young workforce, with 62.5% below the age of 40, indicating a predominance of early-to-mid career professionals who may be more familiar with emerging technologies. Educational levels were generally high, with over half holding university undergraduate degrees (51.5%), and an additional 29.4% having college qualifications, supporting the assumption that KLIA's crisis management and technology-related roles require substantial educational preparation.

Table 2. Demographic Profile of Respondents (N = 136)

Variable	Group	Frequency	Percent (%)
Gender	Male	86	63.2
	Female	50	36.8
	Total	**136**	**100**
Age	Under 29	40	29.4
	30–39	45	33.1
	40–49	25	18.4
	50–59	16	11.8
	Over 60	10	7.4
	Total	**136**	**100**
Education	University Undergraduate	70	51.5
	College	40	29.4
	Masters	6	4.4
	PhD	4	2.9
	Others	16	11.8
	Total	**136**	**100**
Work Type	Full-time	110	80.9
	Part-time	26	19.1
	Total	**136**	**100**
Experience	1–5 years	50	36.8

Variable	Group	Frequency	Percent (%)
	6–9 years	30	22.1
	10 years or above	56	41.2
	Total	**136**	**100**
Job Title	Employee	65	47.8
	Technology Experts	20	14.7
	Crisis Management Specialists	20	14.7
	Organizational Leaders	15	11.0
	Others	16	11.8
	Total	**136**	**100**

Most respondents were full-time employees (80.9%), increasing the reliability of responses because full-time staff are typically more engaged in operational and crisis management activities. Work experience was well distributed: 41.2% had ten or more years, while 36.8% had 1–5 years, providing a balanced mix of senior and junior professionals. In terms of job roles, nearly half were general employees (47.8%), supplemented by specialized groups including technology experts (14.7%), crisis management specialists (14.7%), and organizational leaders (11%). This distribution ensures that the dataset captures diverse operational, technical, and managerial perspectives relevant to drone threat management at KLIA.

Evaluation of the Research Model

This study employed Partial Least Squares Structural Equation Modelling (PLS-SEM) to assess the relationships within the proposed framework, which includes the effects of technology readiness and technology usage on crisis management effectiveness at KLIA. PLS-SEM is well suited for analysing complex models involving multiple latent constructs and is particularly useful when working with modest sample sizes or when the research includes constructs measured through several indicators (Hair et al., 2019). In this study, the technique enabled the estimation of both direct and mediating relationships among the variables, providing insights into how well the model explains crisis management outcomes. The analysis followed the standard two-step procedure, beginning with the evaluation of the measurement model to ensure reliability and validity, followed by the assessment of the structural model to test the hypothesized relationships. All analyses were conducted using the SmartPLS software, and the results of these procedures are presented in the following sections.

Stage 1: Measurement model assessment

The first stage of the PLS-SEM analysis involved evaluating the measurement model to confirm the reliability and validity of the constructs used in this study. Following established guidelines (Cheung et al., 2023; Henseler et al., 2015), three key criteria were assessed: convergent validity, internal consistency reliability, and discriminant validity. Convergent validity was examined through the Average Variance Extracted (AVE) and indicator loadings. As recommended, AVE values exceeded the minimum threshold of 0.50 for all constructs, confirming that each construct explains more than half of the variance in its indicators. Similarly, most item loadings surpassed 0.70, indicating that the items strongly represent their respective latent variables. Items with poor loadings such as CM5, CM6, TR-IP5, and TR-PP1 were removed to improve construct quality.

Internal consistency reliability was confirmed through Cronbach's Alpha (CA) and Composite Reliability (CR). All CA values were above 0.80, and CR values exceeded 0.90, demonstrating strong reliability across constructs including Crisis Management, Technology Readiness dimensions (Infrastructure Preparedness, Policy & Procedures, Staff Training, Technology Adoption), and Technology Usage.

Table 3. The outer loadings for each indicator in the initial and revised models

Construct	Indicator	Initial	Revised	CA	CR	(AVE)
Crisis Management	CM1	0.844	0.846	0.899	0.929	0.766
	CM2	0.892	0.891			
	CM3	0.933	0.934			
	CM4	0.825	0.825			

Construct	Indicator	Initial	Revised	CA	CR	(AVE)
	CM5	0.169	Deleted			
	CM6	-0.058	Deleted			
Technology Readiness–Infrastructure Preparedness	TR-IP1	0.822	0.823	0.920	0.944	0.809
	TR-IP2	0.958	0.959			
	TR-IP3	0.848	0.847			
	TR-IP4	0.959	0.959			
	TR-IP5	0.045	Deleted			
Technology Readiness–Policy and Procedures	TR-PP1	0.513	Deleted	0.929	0.949	0.825
	TR-PP2	0.904	0.905			
	TR-PP3	0.885	0.884			
	TR-PP4	0.913	0.912			
	TR-PP5	0.929	0.930			
Technology Readiness–Staff Training	TR-ST1	0.880	0.880	0.891	0.919	0.696
	TR-ST2	0.824	0.824			
	TR-ST3	0.828	0.828			
	TR-ST4	0.886	0.886			
	TR-ST5	0.745	0.745			
Technology Readiness–Technology Adoption	TR-TA1	0.833	0.833	0.899	0.923	0.706
	TR-TA2	0.824	0.824			
	TR-TA3	0.795	0.795			
	TR-TA4	0.891	0.891			
	TR-TA5	0.854	0.854			
Technology Usage	TU1	0.841	0.842	0.860	0.895	0.631
	TU2	0.816	0.816			
	TU3	0.753	0.752			
	TU4	0.711	0.710			
	TU5	0.843	0.843			

Table 3 summarises the final indicator loadings, reliability coefficients, and AVE values after revision. The consistently high CA, CR, and AVE values confirm that the remaining indicators accurately capture the constructs and meet the recommended psychometric standards. These results provide confidence in the robustness of the measurement model and its suitability for subsequent structural analysis.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

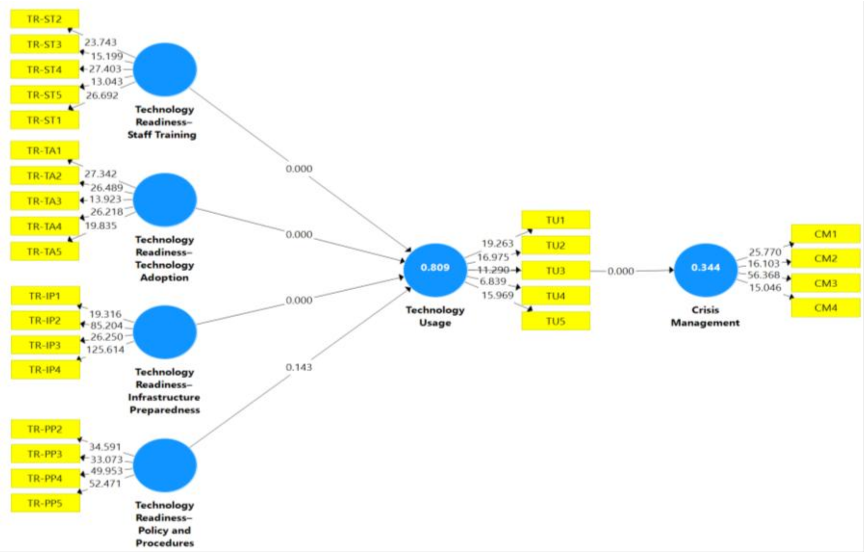


Figure 3. Structural model for the direct and mediating effects

Discriminant Validity Assessment (Fornell–Larcker Criterion)

Discriminant validity was evaluated using the Fornell and Larcker (1981) criterion, which compares the square root of the AVE for each construct with the correlations between that construct and all others. Table 4 presents the results, with the diagonal values representing the square root of AVE and the off-diagonal values showing the inter-construct correlations.

Table 4. Results of the discriminant validity using the Fornell and Larker's Criterion

Construct	CM	TR-IP	TR-PP	TR-ST	TR-TA	TU
CM	0.875					
TR-IP	0.692	0.899				
TR-PP	0.301	0.598	0.908			
TR-ST	0.255	0.545	0.526	0.834		
TR-TA	0.707	0.636	0.354	0.198	0.840	
TU	0.597	0.808	0.539	0.489	0.801	0.794

** Note: Table.4 Diagonal elements highlighted in boxes represent the square root of AVE, and the off-diagonal elements are a bivariate correlation between constructs.

The results indicate that, for all constructs Crisis Management (CM), Technology Readiness dimensions (Infrastructure Preparedness, Policy & Procedures, Staff Training, Technology Adoption), and Technology Usage the square root of the AVE (diagonal values) is greater than the corresponding inter-construct correlations. For example, the square root of AVE for Technology Usage (0.794) exceeds its correlations with other constructs, including TR-IP (0.808) and TR-TA (0.801). Similarly, Crisis Management (0.875) shows higher diagonal values compared to its correlations with TR-IP (0.692) and TR-TA (0.707).

These results confirm that each construct shares more variance with its own indicators than with other constructs in the model. Therefore, the requirements for discriminant validity are satisfied, supporting the conclusion that the constructs are conceptually distinct and appropriately measured within this study.

Stage 2: Structural Model Assessment

Following the confirmation of the measurement model, the analysis proceeded to the structural model assessment, which evaluates the hypothesized relationships among the constructs and determines the predictive power of the research model. This stage involved examining path coefficients, p-values, and the overall significance of direct and mediating effects to test the study's hypotheses.

Direct Effects

Table 5 presents the results for the direct relationships. Technology Usage demonstrated a strong and significant positive effect on Crisis Management (β = 0.587, p < 0.001), supporting H1 and confirming its central role in enhancing KLIA's ability to manage drone-related crises. Among the technology readiness components, Infrastructure Preparedness (β = 0.304, p < 0.001), Staff Training (β = 0.166, p < 0.001), and Technology Adoption (β = 0.567, p < 0.001) all had significant positive effects on Technology Usage, supporting H2, H4, and H5 respectively. However, Policy and Procedures showed no significant relationship with Technology Usage (β = 0.056, p = 0.143), resulting in H3 not being supported. This indicates that formal policies alone do not directly influence the extent to which technology is used in drone threat management at KLIA.

Table 5. Path coefficient assessment direct relationship (N=136)

Hyp.	Relationship	β	P Values	Results
H1	Technology Usage -> Crisis Management	0.587	0.000	Supported
Technology Readiness				
H2	Infrastructure Preparedness -> Technology Usage	0.304	0.000	Supported
H3	Policy and Procedures -> Technology Usage	0.056	0.143	Not Supported
H4	Staff Training -> Technology Usage	0.166	0.000	Supported
H5	Technology Adoption -> Technology Usage	0.567	0.000	Supported

Mediating Effects

Table 6 displays the mediating relationships, where Technology Usage functions as the mediator between technology readiness components and Crisis Management. Significant mediation was found for Infrastructure Preparedness (β = 0.179, p < 0.001), Staff Training (β = 0.097, p < 0.001), and Technology Adoption (β = 0.333, p < 0.001), supporting H6, H8, and H9. These results indicate that the positive influence of these readiness factors on Crisis Management operates largely through their effect on Technology Usage. Conversely, Policy and Procedures did not exhibit a significant mediating effect through Technology Usage (β = 0.033, p = 0.147), meaning H7 was not supported. This further reinforces the limited role of procedural documentation in driving operational effectiveness during drone crises unless supported by active technological engagement.

Table 6. Path coefficient assessment mediating relationship (N=136)

Hyp.	Relationship	β	P Values	Results
Technology Readiness				
H6	Infrastructure Preparedness -> Technology Usage -> Crisis Management	0.179	0.000	Supported
H7	Policy and Procedures -> Technology Usage -> Crisis Management	0.033	0.147	Not Supported
H8	Staff Training -> Technology Usage -> Crisis Management	0.097	0.000	Supported
H9	Technology Adoption -> Technology Usage -> Crisis Management	0.333	0.000	Supported

Overall, the structural model results underscore the importance of technology-driven operational readiness, highlighting Technology Usage as a crucial mechanism that links readiness components particularly infrastructure, staff capability, and technology adoption to effective crisis management at KLIA.

DISCUSSION

The findings demonstrate that technology readiness plays a critical role in shaping KLIA's ability to manage drone-related crises, with the most influential factors being technology adoption and infrastructure preparedness, followed by staff training. These results reinforce prior work highlighting that adopting advanced technologies such as drone detection radars, geofencing, and AI-based surveillance is essential for mitigating risks posed by UAVs (Backman & Rhinard, 2018; Mohsan et al., 2023). Similarly, the strong impact of infrastructure preparedness supports earlier studies emphasizing that robust technological systems and operational infrastructures significantly enhance airports'

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

crisis response capabilities (Hodgkinson & Johnston, 2018; Matysek & Wojakowska, 2023; Price & Forrest, 2016). Staff training, though less influential, remains important because technological tools are only as effective as the personnel operating them, consistent with Parasuraman's (2000) and Testoni et al. (2021) view of human readiness as a core component of crisis management capability. In contrast, policy and procedures showed no significant direct effect, suggesting that formal guidelines alone do not translate into operational readiness without meaningful adoption, infrastructure support, and training echoing prior critiques that practical implementation is more crucial than policy presence (Hodgkinson & Johnston, 2018; Mizrak, 2024).

Technology usage itself showed a strong direct influence on crisis management, confirming that effective utilization of technological tools enhances detection, situational awareness, and response coordination during drone incidents. This aligns with research emphasizing that UAV threats require real-time technological interventions (Perz, 2024; Singh, 2024). It also supports the Situational Crisis Communication Theory (SCCT), which stresses that effective crisis response mechanisms strengthen organizational resilience and protect operational continuity (Coombs, 2007).

The mediating analysis further revealed that technology usage acts as a central mechanism linking technology readiness factors infrastructure, training, and adoption to crisis management outcomes. This indicates that readiness must be operationalized through active technology utilization, consistent with the argument that training, adoption, and infrastructure are meaningful only when embedded in daily practice (Parasuraman, 2000; Sharma & Venkatraman, 2023; Testoni et al., 2021). Policy and procedures did not exhibit a meaningful mediation effect, reinforcing that governance frameworks require practical technological engagement to influence outcomes.

Based on these insights, the study proposes a structured framework emphasizing three pillars: advanced technology adoption, infrastructure resilience, and continuous staff training, complemented by supportive but not determinative policy alignment. This integrated approach reflects international recommendations for strengthening aviation security against UAV threats (Backman & Rhinard, 2018; Eleimat et al., 2024; ICAO, 2025). Overall, the findings highlight that KLIA's drone crisis management effectiveness depends not on procedural formality but on practical technological readiness, operational deployment, and competent human resources.

CONCLUSION

This study explored how technology readiness and technology usage contribute to crisis management effectiveness at Kuala Lumpur International Airport (KLIA), with a specific focus on emerging drone-related threats. The key findings show that technology adoption, infrastructure preparedness, and staff training are the most influential readiness dimensions, whereas policy and procedures alone do not significantly enhance technology usage or crisis outcomes. Technology usage itself demonstrated a strong direct effect on crisis management, confirming that the actual utilization of technological tools is essential for improving response capabilities. Mediation analysis further revealed that technology usage is the primary mechanism through which readiness factors translate into effective crisis management, underscoring the importance of operational implementation rather than reliance on procedural frameworks.

The demographic composition of respondents representing diverse experience levels and job roles provided a comprehensive view of readiness and crisis management practices across KLIA's workforce. The validated measurement and structural models further confirmed the robustness of the research framework. Based on these insights, the study proposed a structured framework emphasizing investment in advanced technologies, resilient infrastructure, continuous staff training, and alignment of policies with practical operations. These pillars collectively strengthen readiness and enhance KLIA's ability to manage drone threats proactively.

Overall, the study concludes that crisis management effectiveness depends largely on how well technology readiness dimensions are operationalized through active technology usage. By highlighting the factors that matter most adoption, infrastructure, and training this research offers valuable theoretical and practical contributions for improving resilience in the aviation sector and provides a foundation for future work on technology-driven crisis management.

REFRENCES

[1] Al Shobaki, M., Abu Amuna, Y., & Abu Naser, S. (2016). Strategic and Operational Planning As Approach for Crises Management Field Study on UNRWA. *International Journal of Information Technology and Electrical Engineering ITEE*, *5*(6), 43–47.

[2] Alam, M. M., Malik, H., Khan, M. I., Pardy, T., Kuusik, A., & Le Moullec, Y. (2018). A survey on the roles of communication technologies in IoT-Based personalized healthcare applications. *IEEE Access*, *6*, 36611–36631. https://doi.org/10.1109/ACCESS.2018.2853148

[3] Alkharusi, H. (2022). A descriptive analysis and interpretation of data from Likert scales in educational and psychological research. *Indian Journal of Psychology and Education*, *12*(2), 13–16.

[4] Amaral, F. (2019). *They have something to say: A study of social media use and public discourse in the Rio de Janeiro favelas*.

[5] Amuna, Y. M. A., Shobaki, M. J. A., & Naser, S. S. A. (2017). Strategic environmental scanning: An approach for crises management. *International Journal of Information Technology and Electrical Engineering*, *6*(3), 28–34.

[6] Arafat, S., Chowdhury, H. R., Qusar, M., & Hafez, M. (2016). Cross cultural adaptation and psychometric validation of research instruments: A methodological review. *Journal of Behavioral Health*, *5*(3), 129–136.

[7] Azizan, A. Z., & Lim, C. C. (2023). A Study of Entrepreneurial Characteristics and Entrepreneurial Intention among Electrical and Electronic Engineering Students. *Research in Management of Technology and Business*, *4*(2), 041–057.

[8] Backman, S., & Rhinard, M. (2018). The European Union's capacities for managing crises. *Journal of Contingencies and Crisis Management*, *26*(2), 261–271. https://doi.org/10.1111/1468-5973.12190

[9] Baker, J. (2012). The Technology–Organization–Environment Framework. In Y. K. Dwivedi, M. R. Wade, & S. L. Schneberger (Eds.), *Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1* (pp. 231–245). Springer. https://doi.org/10.1007/978-1-4419-6108-2_12

[10] Balci, H. (2023). *The use of drones in airport security operations*.

[11] Bennett, D. (2019). Information and Communication Technology in Crisis and Disaster Management. *Oxford Research Encyclopedia of Politics*. https://doi.org/10.1093/acrefore/9780190228637.013.1582

[12] Bolt, B. A., Horn, W., MacDonald, G. A., & Scott, R. (2013). *Geological Hazards: Earthquakes-tsunamis-volcanoes-avalanches-landslides-floods*. Springer Science & Business Media.

[13] Bongiovanni, I., & Newton, C. (2019). Toward an epidemiology of safety and security risks: An organizational vulnerability assessment in international airports. *Risk Analysis*, *39*(6), 1281–1297.

[14] Bougie, R., & Sekaran, U. (2019). *Research methods for business: A skill building approach*. john wiley & sons.

[15] Brown, A. J., Korza, A. G., Donahue, J., Parnas, L. N., & Borowski, N. M. (2016). *The Drone Perspective-A research project exploring the advancement of the commercial drone industry and its effect on society*.

[16] Calandrillo, S., Oh, J., & Webb, A. (2020). Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety. *Stanford Technology Law Review*, *23*, 182–252.

[17] Cheung, G. W., Cooper-Thomas, H. D., Lau, R. S., & Wang, L. C. (2023). Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. *Asia Pacific Journal of Management*, 1–39.

[18] Comes, T., Meesters, K., & Torjesen, S. (2019). Making sense of crises: The implications of information asymmetries for resilience and social justice in disaster-ridden communities. *Sustainable and Resilient Infrastructure*, *4*(3), 124–136. https://doi.org/10.1080/23789689.2017.1405653

[19] Cook, N. S., Cave, J., & Holtorf, A. P. (2019). Patient preference studies during early drug development: Aligning stakeholders to ensure development plans meet patient needs. *Frontiers in Medicine*, *6*(APR). https://doi.org/10.3389/fmed.2019.00082

[20] Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, *10*(3), 163–176.

[21] Department of Homeland Security, U. (2023). *Virtual Reality (VR) Training Systems for First Responders Market Survey Report*.

[22] Dias, C. A. S. (2024). *Smart Airports: Analysing Digital Transformation and Technological Advancements in Aviation*.

[23] Dudenhoeffer, D. D. (2020). Day of the drone: Protecting critical infrastructure from terrorist use of unmanned aerial systems. In *Toward Effective Cyber Defense in Accordance with the Rules of Law* (pp. 17–31). IOS Press.

[24] Dulaney, E., & Gunn, R. (2017). Situational crisis communication theory and the use of apologies in five high-profile food-poisoning incidents. *Journal of the Indiana Academy of the Social Sciences*, *20*(1), 5.

[25] EASA. (2021). *Drones & Air Mobility*. https://www.easa.europa.eu/en/domains/civil-drones

[26] Eleimat, M., Alharasees, O., & Oszi, A. (2024). *Advancements in airport security technologies: A patent analysis*. 1–5.

[27] Erdfelder, E., FAul, F., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

[28] Grand View Research. (2025). *Drone Market Size, Share & Growth | Industry Report, 2030*. https://www.grandviewresearch.com/industry-analysis/drone-market-report

[29] Hair, J. F., Page, M., & Brunsveld, N. (2019). *Essentials of business research methods*. Routledge.

[30] Hauberg, J. (2011). Research by design: A research strategy. *Revista Lusófona de Arquitectura e Educação*.

[31] Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*, 115–135.

[32] Hern, A., & Topham, G. (2018). How dangerous are drones to aircraft? *The Guardian*.

[33] Hodgkinson, D., & Johnston, R. (2018). *Aviation law and drones: Unmanned aircraft and the future of aviation*. Routledge.

[34] ICAO. (2025). *Workshop on Drone Operations, Challenges and Opportunities for NAM/CAR/SAM Regions Mexico City, Mexico, 17 to 19 June 2025*. International Civil Aviation Organization. https://www2023.icao.int/NACC/Pages/meetings-2025-wdoco.aspx

[35] Keller, E. A., DeVecchio, D. E., & Clague, J. J. (2016). Natural hazards: Earth's processes as hazards, disasters, and catastrophes. *Natural Hazards: Earth's Processes as Hazards, Disasters, and Catastrophes*, 1–488. https://doi.org/10.4324/9781315269160

[36] Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

[37] Matović, N., & Ovesni, K. (2023). Interaction of quantitative and qualitative methodology in mixed methods research: Integration and/or combination. *International Journal of Social Research Methodology*, *26*(1), 51–65. https://doi.org/10.1080/13645579.2021.1964857

[38] Matysek, K., & Wojakowska, M. (2023). Airport security management in the context of fire protection on the example of the Chopin Airport in Warsaw. *Zeszyty Naukowe SGSP/Szkoła Główna Służby Pożarniczej*.

[39] McCaffrey, S., McGee, T. K., Coughlan, M., & Tedim, F. (2020). Understanding wildfire mitigation and preparedness in the context of extreme wildfires and disasters: Social science contributions to understanding human response to wildfire. In *Extreme wildfire events and disasters* (pp. 155–174). Elsevier.

[40] McLeod, S., & Curtis, C. (2020). Understanding and Planning for Freight Movement in Cities: Practices and Challenges. *Planning Practice and Research*, *35*(2), 201–219. https://doi.org/10.1080/02697459.2020.1732660

[41] Mijović, V., Tomašević, N., Janev, V., Stanojević, M., & Vraneš, S. (2019). Emergency management in critical infrastructures: A complex-event-processing paradigm. *Journal of Systems Science and Systems Engineering*, *28*(1), 37–62.

[42] Miles, M. B. (1994). Qualitative data analysis: An expanded sourcebook. *Thousand Oaks*.

[43] Mizrak, K. C. (2024). Crisis management and risk mitigation: Strategies for effective response and resilience. *Trends, Challenges, and Practices in Contemporary Strategic Management*, 254–278.

[44] Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intelligent Service Robotics*, *16*(1), 109–137.

[45] National Academies of Sciences. (2025). *Collaborative for Advancing Science Teaching and Learning in K-12*. https://www.nationalacademies.org/our-work/collaborative-for-advancing-science-teaching-and-learning-in-k-12

[46] News, B. B. C. (2018). *Drones ground flights at Gatwick*. BBC News.

[47] Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, *14*(1), pp110-121.

[48] Parasuraman, A. (2000). Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies. *Journal of Service Research*, *2*(4), 307–320.

[49] Parker, C. F., Nohrstedt, D., Baird, J., Hermansson, H., Rubin, O., & Baekkeskov, E. (2020). Collaborative crisis management: A plausibility probe of core assumptions. *Policy and Society*, *39*(4), 510–529. https://doi.org/10.1080/14494035.2020.1767337

[50] Pedersen, C. L., Ritter, T., & Di Benedetto, C. A. (2020). Managing through a crisis: Managerial implications for business-to-business firms. *Industrial Marketing Management*, *88*, 314–322. https://doi.org/10.1016/j.indmarman.2020.05.034

[51] Perz, R. (2024). The multidimensional threats of un-manned aerial systems: Exploring biomechanical, technical, operational, and legal solutions for ensuring safety and security. *Archives of Transport*, *69*(1), 91–111.

[52] Plotnick, L., & Hiltz, S. R. (2018). Software Innovations to Support the Use of Social Media by Emergency Managers. *International Journal of Human-Computer Interaction*, *34*(4), 367–381. https://doi.org/10.1080/10447318.2018.1427825

[53] Price, J., & Forrest, J. (2016). *Practical airport operations, safety, and emergency management: Protocols for today and the future*. Butterworth-Heinemann.

[54] Pyrgies, J. (2019). The UAVs threat to airport security: Risk analysis and mitigation. *Journal of Airline and Airport Management*, *9*(2), 63–96.

[55] Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, *6*(2), 1–5.

[56] Raspotnig, C., Karpati, P., & Opdahl, A. L. (2020). Combined assessment of software safety and security requirements: An industrial evaluation of the chassis method. *Research Anthology on Artificial Intelligence Applications in Security*, *2–4*, 666–693. https://doi.org/10.4018/978-1-7998-7705-9.ch031

[57] Regmi, P. R., Waithaka, E., Paudyal, A., Simkhada, P., & Van Teijlingen, E. (2016). Guide to the design and application of online questionnaire surveys. *Nepal Journal of Epidemiology*, *6*(4), 640.

[58] Reitz, F. (2025, February 6). Unruly Passengers: The Growing Challenge for Airline Security Part one: Understanding the Problem. *Transport Security International Magazine*. https://tsi-mag.com/unruly-passengers-the-growing-challenge-for-airline-security-part-one-understanding-the-problem/

[59] Ritchie, B. W., & Jiang, Y. (2019). A review of research on tourism risk, crisis and disaster management: Launching the annals of tourism research curated collection on tourism risk, crisis and disaster management. *Annals of Tourism Research*, *79*. https://doi.org/10.1016/j.annals.2019.102812

[60] Saad, W., Bennis, M., Mozaffari, M., & Lin, X. (2020). *Wireless communications and networking for unmanned aerial vehicles*. Cambridge University Press.

[61] Samaan, J. L. C. (2020). Missiles, drones, and the houthis in yemen. *Parameters*, *50*(1), 51–63.

[62] Sammler, K. G., & Lynch, C. R. (2021). Spaceport America: Contested Offworld Access and the Everyman Astronaut. *Geopolitics*, *26*(3), 704–728. https://doi.org/10.1080/14650045.2019.1569631

[63] Sandbrook, C. (2015). The social implications of using drones for biodiversity conservation. *Ambio*, *44*, 636–647. https://doi.org/10.1007/s13280-015-0714-0

[64] Sandin, P. (2018). Conceptualizations of Disasters in Philosophy. *Advancing Global Bioethics*, *11*, 13–26. https://doi.org/10.1007/978-3-319-92722-0_2

[65] Saroj, A., & Pal, S. (2020). Use of social media in crisis management: A survey. *International Journal of Disaster Risk Reduction*, *48*(April), 101584. https://doi.org/10.1016/j.ijdrr.2020.101584

[66] Schröter, E., Kiefl, R., Neidhardt, E., Gurczik, G., Dalaff, C., & Lechner, K. (2020). Trialing innovative technologies in crisis management-"airborne and terrestrial situational awareness" as support tool in flood response. *Applied Sciences (Switzerland)*, *10*(11). https://doi.org/10.3390/app10113743

[67] Sciancalepore, S., Ibrahim, O. A., Oligeri, G., & Di Pietro, R. (2019). *Detecting drones status via encrypted traffic analysis*. 67–72.

[68] Sharma, A., & Venkatraman, S. (2023). Towards a standard framework for organizational readiness for technology adoption. In *Advances in digital manufacturing systems: Technologies, business models, and adoption* (pp. 197–219). Springer.

[69] Singh, B. (2024). Unmanned aircraft systems (UAS), surveillance, risk management to cybersecurity and legal regulation landscape: Unraveling the future analysis, challenges, demand, and benefits in the high sky exploring the strange new world. *Unmanned Aircraft Systems*, 313–354.

[70] Tagarev, T., & Ratchev, V. (2020). A taxonomy of crisis management functions. *Sustainability*, *12*(12), 5147.

[71] Testoni, R., Bersano, A., & Segantin, S. (2021). Review of nuclear microreactors: Status, potentialities and challenges. *Progress in Nuclear Energy*, *138*, 103822. https://doi.org/10.1016/J.PNUCENE.2021.103822

[72] Varma, T. (2019). Understanding Decision Making During a Crisis: An Axiomatic Model of Cognitive Decision Choices. *International Journal of Business Communication*, *56*(2), 233–248. https://doi.org/10.1177/2329488415612477

[73] Waryjas, M. A. (1999). *EFFECTIVE CRISIS MANAGEMENT: Grace Under Pressure*.

[74] Weaver, M., Gayle, D., Greenfield, P., & Perraudin, F. (2018). Military called in to help with Gatwick drone crisis. *The Guardian*.

[75] White, C. M. (2011). *Social media, crisis communication, and emergency management: Leveraging Web 2.0 technologies*. CRC press.

[76] Wright, D. (2014). Drones: Regulatory challenges to an incipient industry. *Computer Law and Security Review*, *30*(3), 226–229. https://doi.org/10.1016/j.clsr.2014.03.009

[77] Zhang, Y., Suhaimi, N., Azghandi, R., Joseph, M. A., Kim, M., Griffin, J., & Parker, A. G. (2020). *Understanding the use of crisis informatics technology among older adults*. 1–13.

[78] Zhu, K., Kraemer, K. L., & Xu, S. (2006). The process of e-business assimilation in organizations: A technology diffusion perspective. *Management Science*, *52*(10), 1557–1576.