Journal of Transportation Security (2026) 19:39
https://doi.org/10.1007/s12198-026-00362-x

RESEARCH

Narratives of protection: assessing the effectiveness of aviation security measures through practitioner storytelling

Hanan China Gahwita[1] · Ekrem Tatoglu[2,3] · Halit Keskin[4] · Ali E. Akgün[4] · Emel Esen[4]

Received: 7 April 2026 / Accepted: 11 July 2026

Abstract

Civil aviation continues to face evolving threats of unlawful interference, including terrorism, hijacking, sabotage, and cyber-enabled attacks. Although regulatory frameworks, technological capabilities, and international cooperation have strengthened considerably, evaluating the effectiveness of aviation security remains largely centered on procedural compliance and incident-based indicators. This study adopts a practice-oriented perspective by examining how aviation security effectiveness is interpreted and assessed by professionals directly involved in implementing security measures. Drawing on in-depth interviews with experienced aviation security and safety practitioners, professional narratives were analyzed thematically to explore how deterrence, vulnerability, and security effectiveness are understood in operational settings. Guided by deterrence theory, the analysis demonstrates that practitioners associate effective security not only with technological capability and regulatory compliance, but also with consistent implementation, professional judgment, organizational coordination, and alignment with international standards, particularly those established by the International Civil Aviation Organization (ICAO). Participants also identified persistent challenges associated with human factors, resource constraints, and evolving threat environments, while emphasizing insider threats as a context-dependent source of vulnerability requiring sustained organizational vigilance. Rather than offering broadly generalizable conclusions, the study provides context-specific insights into how deterrence is interpreted and enacted in contemporary aviation practice. In doing so, it complements predominantly technical and regulatory perspectives by highlighting the value of practitioner narratives for informing future research, operational decision-making, and policy discussions concerning aviation security.

Keywords Aviation security · Transport security · Unlawful interference · Deterrence theory · Qualitative research · Practitioner narratives

Extended author information available on the last page of the article

Published online: 21 July 2026

Introduction

Aviation plays a central role in global connectivity by enabling the movement of people and goods across long distances and supporting international economic and social interaction (Adey et al. 2007). Owing to its complex operational structure and high passenger density, safety and security have long remained fundamental priorities within the aviation industry (Oster et al. 2013; Wong et al., 2015). At the same time, the sector continues to face evolving forms of unlawful interference, including terrorism, cyber-attacks, sabotage, and the smuggling of dangerous goods (Abeyratne 2011; Klenka 2021; Fox 2016; Huang et al. 2020). The adaptive nature of these threats requires security frameworks that evolve alongside changing operational risks while maintaining the efficiency and integrity of global air transport (Abeyratne & Abeyratne 2020).

The importance of aviation security becomes particularly apparent when examined through major historical incidents that have shaped regulatory and operational practices (Dawson 1987; Harrison 2009). The terrorist attacks of September 11, 2001, demonstrated how commercial aircraft could be exploited as weapons, fundamentally altering global perceptions of aviation vulnerability and the governance of civil aviation security (Arasly 2005). Beyond their immediate human and economic consequences, the attacks accelerated a transition toward a more preventive, intelligence-led, and globally coordinated aviation security regime that continues to shape contemporary policy and operational practice nearly twenty-five years later (Salter 2008; Sinai 2012). Often described as "the day that changed the world," these attacks resulted in unprecedented loss of life and marked a turning point in aviation security governance (Fox 2021). Governments and aviation authorities, working in coordination with the International Civil Aviation Organization (ICAO), subsequently introduced enhanced passenger screening procedures, reinforced cockpit doors, advanced travel document verification, full-body scanners, and no-fly lists (Fox 2021; ICAO, 2017). These developments marked not simply the expansion of security technologies, but the institutionalization of a layered security philosophy intended to deter, detect, and prevent unlawful interference across multiple stages of the passenger journey. Collectively, these developments established a preventive, intelligence-informed, and internationally coordinated model of aviation security governance that continues to underpin contemporary operational practice nearly twenty-five years after the September 11 attacks.

Earlier incidents had already exposed structural weaknesses within aviation security systems. The bombing of Air India Flight 182 in 1985, which claimed the lives of all 329 passengers and crew, revealed critical shortcomings in baggage screening and intelligence coordination (Price and Forrest 2016). The simultaneous bombing attempt at Tokyo's Narita International Airport further emphasized the need for more comprehensive airport security procedures (Roach 2011). Subsequent investigations identified limitations in pre-flight explosive detection and failures in intergovernmental communication as key enabling factors (Britannica, 2023; The Canadian Encyclopedia, 2023). Similarly, the bombing of Pan Am Flight 103 over Lockerbie in 1988 illustrated the consequences of inadequate detection technologies, as the concealed SEMTEX explosive evaded the screening methods available at the

time. Beyond its tragic human consequences, the Lockerbie disaster became a catalyst for major regulatory and technological reforms, accelerating international efforts to strengthen baggage screening, explosive detection, and intelligence cooperation (Baker 2020; Jenkins 2017).

Despite significant advancements since these events, later incidents indicate that aviation security threats have not disappeared but have instead diversified (Harrison 2009). The attempted shoe-bomb attack in 2001 exposed vulnerabilities in passenger screening practices and led to the introduction of additional security requirements, including shoe removal during screening processes (Jager 2018). More recently, the coordinated shooting and bombing attack at Istanbul Atatürk Airport in 2016 demonstrated that aviation terrorism extends beyond aircraft to encompass airport terminals and landside areas (Duchesneau and Langlois 2017). This incident reinforced the symbolic and strategic value of aviation infrastructure as a target, while also revealing broader social and economic consequences for transit hubs and tourism-dependent economies (Uzulmez & Ates 2017).

Existing scholarship frequently portrays aviation terrorism as a symbolic form of violence intended to generate global media attention, political pressure, and widespread public fear (Altheide 2007; Tuman 2009). Aviation remains an attractive target due to its international visibility and the significant economic and reputational damage associated with successful attacks (Glen 2014; Krull 2016). Earlier periods marked by frequent hijackings and armed seizures of aircraft, particularly between the 1930 s and 1980 s, illustrate how limited detection technologies and underdeveloped security frameworks contributed to the prevalence of unlawful interference acts (Arasly 2005). Although aviation security has undergone substantial transformation since 9/11, these historical developments demonstrate that unlawful interference continues to evolve alongside technological, organizational, and geopolitical change. Consequently, understanding security effectiveness requires attention not only to technological capability but also to the ways in which protective measures are interpreted and implemented in practice (Schober et al., 2012; Baker 2020).

While existing scholarship has generated important insights into aviation security through analyses of regulatory frameworks, technological developments, and major incidents, much of this literature remains primarily event-driven or technically oriented. Consequently, comparatively limited attention has been devoted to how the effectiveness of post-9/11 aviation security systems is interpreted, experienced, and operationalized by the professionals responsible for implementing protective measures in everyday operational settings (Price and Forrest 2024). Although deterrence is widely treated as a relevant concept in aviation security research, less is known about how security measures are understood by practitioners in relation to perceived detection risk, uncertainty, and behavioral restraint in operational environments. This limitation is particularly important in contemporary aviation environments characterized by layered security architectures, organizational complexity, and continuously evolving threat conditions. In parallel, the organizational and human dimensions of aviation security, particularly how personnel experience, interpret, and implement security protocols in practice, continue to receive limited scholarly attention (Hall et al. 2022).

Addressing these gaps, the present study examines aviation security measures as both protective and deterrent mechanisms from the perspective of aviation security professionals. Rather than assessing offender behavior directly, the analysis draws on historical incidents, contemporary security practices, and professional narratives to investigate how security effectiveness and deterrence are interpreted and enacted within aviation settings. Emphasis is placed on practitioner sensemaking and experiential knowledge to provide an exploratory, practice-oriented perspective on how security measures are understood and implemented within contemporary civil aviation systems. Accordingly, attention is directed toward how aviation security professionals evaluate current protective practices, deterrence mechanisms, implementation challenges, and emerging vulnerabilities within increasingly complex operational environments.

RQ1. How do aviation security professionals assess the effectiveness of current aviation security measures in preventing and mitigating acts of unlawful interference?
RQ2. How do aviation security professionals perceive the role of deterrence, coordination, and information sharing in contemporary aviation security practices?
RQ3. How do aviation security professionals evaluate current challenges, emerging threats, and potential improvements in aviation security systems?

Addressing these questions, the study provides exploratory insights into how aviation security professionals understand security effectiveness, deterrence, and implementation challenges in everyday practice. In doing so, it complements predominantly technical and regulatory perspectives by incorporating practitioner experience into contemporary discussions of aviation security governance. The findings also offer practical implications for aviation managers, policymakers, and regulatory authorities seeking to balance security requirements, operational efficiency, and passenger experience within increasingly complex aviation environments (Jackson et al. 2012; Merhi and Ahluwalia 2019; Stewart and Mueller 2011).

Literature review

Research on aviation security spans a broad range of themes, including evolving threat environments, technological and organizational countermeasures, policy evaluation, and behavioral responses to security interventions. Existing studies reflect sustained concern with how aviation systems can prevent unlawful interference while maintaining operational reliability and public legitimacy. To provide a coherent foundation for the present study, this section first reviews research on aviation security measures and their adaptation to changing threat conditions. It then considers deterrence theory as an analytical perspective for examining how security measures may influence offender perceptions and behavior within the broader operational and policy context of civil aviation.

Aviation security measures and evolving threat environments

Aviation security is widely recognized as a prerequisite for the continuity, legitimacy, and operational reliability of air transport (Pettersen and Bjørnskau 2015). Aviation systems combine high passenger volumes, complex infrastructure, time sensitive operations, and international connectivity, which exposes them to a wide range of unlawful interference, including terrorism, hijacking, sabotage, cyber-attacks, and the movement of prohibited or dangerous items (National Research Council, 2002). Prior research emphasizes that the continuing diversification of these threats has required ongoing adaptation of security strategies, operational procedures, and technological capabilities aimed at preventing, detecting, and mitigating unlawful interference (Abeyratne & Abeyratne 2020). At the same time, effective aviation security is increasingly understood to extend beyond technological solutions and encompass policy choices, organizational routines, human enforcement, passenger compliance, and the continual balancing of protection with operational efficiency and public legitimacy.

A substantial body of research documents the portfolio of aviation security measures and evaluates their operational strengths and limitations. Studies frequently describe aviation security as a multi-layered system that integrates screening technologies, surveillance and monitoring, access control, threat assessment, and procedural enforcement (Farhaoui et al. 2024). Screening remains one of the most visible and institutionalized components of aviation security. Technologies such as advanced X-ray scanners, metal detectors, and explosive trace detection systems are widely discussed as mechanisms that support the identification of unlawful items and substances. Existing evidence suggests that screening procedures can disrupt threat attempts, although capabilities require continuous updating to address evolving tactics (Stewart & Mueller, 2008). Risk-based approaches, including profiling technologies and behavioral indicators, are also discussed as tools that enable earlier identification of higher-risk individuals and targeted intervention (Klenka 2019). Intelligence-informed and data-driven threat assessments are similarly emphasized as critical for anticipating vulnerabilities and reducing exposure to emerging hazards.

Another recurring theme concerns attacker adaptation. Research suggests that adversaries respond dynamically to security environments and adjust tactics based on the measures they encounter or expect to encounter (Jackson et al. 2007). This observation supports the view that aviation security cannot be treated as static compliance but must be understood as an adaptive system that evolves alongside threat trajectories. Accordingly, prior studies emphasize the importance of continuous evaluation of security measures and institutional learning from both failures and successful interventions (Lacey 2010). This adaptive perspective also highlights the value of collaboration and information sharing among stakeholders across jurisdictions.

Policy and practice considerations form an integral part of aviation security research. Studies emphasize that decision-makers must allocate resources under conditions of uncertainty and constraint, which increases the importance of evidence on which measures provide the greatest security value and under what conditions. Evidence-based security management is often presented as a response to concerns that

without systematic evaluation, investments may be misdirected, and vulnerabilities may remain unaddressed. Research highlights the importance of assessing both operational effectiveness and cost-effectiveness, particularly for advanced imaging and screening technologies that impose substantial financial and organizational demands (Stewart and Mueller 2011). Related work positions systematic evaluation as central to improving the effectiveness and efficiency of aviation security programs (Jackson et al. 2012). This emphasis aligns with broader policy discussions that call for security procedures to balance robust protection with the efficient flow of air traffic (Merhi and Ahluwalia 2019). In operational terms, policymakers are often described as benefiting from guidance on which practices should be maintained, modified, or discontinued as threats evolve and how standards can be harmonized across systems and technologies (Klenka 2019).

Research also addresses the growing role of technology and the tensions it introduces. The expansion of surveillance systems and data management tools can strengthen detection and response capacity, yet it also raises legal and ethical concerns. Studies emphasize that technological deployment must align with legislation and the protection of passenger and worker rights, particularly as security practices become increasingly data intensive (Yao et al. 2012). In this context, innovation is often framed as necessary but insufficient, as advances in detection require complementary governance arrangements, accountability mechanisms, and legitimate implementation.

Motives and tactics of offenders remain another central focus. Scholars argue that effective prevention depends on understanding why individuals or groups engage in unlawful interference and how such acts are operationalized. Motives may include ideological, political, economic, or personal drivers, ranging from extremist objectives to coercive goals, ransom seeking, or retaliatory sabotage (Klenka 2019). Tactics are described as increasingly hybrid, extending from physical smuggling of weapons and explosives to cyber methods targeting airline systems or air traffic control networks (Agustini et al. 2021). Research also suggests that deterrence dynamics may differ depending on whether threats are posed by individuals or organized groups, since organizational structures, strategic calculations, and risk tolerances vary across actor types (Morral et al., 2014).

Public awareness and passenger participation are also discussed as additional layers of aviation security. Informed passengers may be better positioned to identify suspicious behavior and report concerns, supporting early detection and prevention (Fox 2020; Huttunen 2021). Communication strategies include traditional mass media channels for broad outreach (Gilliam Jr 2019) as well as digital platforms for more targeted engagement. Collaboration with businesses, non-governmental organizations, and educational institutions is also highlighted as a means of fostering security awareness through workshops and seminars (Kaunert et al. 2022; Juvan et al. 2021). Research also identifies constraints such as information overload and misinformation, which can reduce trust and weaken the effectiveness of awareness initiatives (Juvan et al. 2021). As a result, targeted communication and attention to legitimacy and rights protection are frequently emphasized (Abeyratne and Abeyratne 2020).

Finally, existing scholarship identifies several gaps that shape ongoing research agendas. One recurring gap concerns the limited number of empirical studies that directly evaluate the effectiveness of specific security procedures in preventing threats and improving aviation safety outcomes (Baker 2020; Juvan et al. 2021). A second gap relates to limited research on psychological drivers and decision mechanisms of perpetrators, which constrains the development of targeted prevention strategies (Huttunen 2021). Another underdeveloped area involves the longer-term impact of security measures on passenger satisfaction and experience, an issue that gains importance as security demands intensify and reshape the passenger journey (Huttunen 2021; Kaunert et al. 2022). These gaps carry direct implications for policy and resource allocation, as limited evaluation complicates prioritization of funding and identification of measures that deliver the greatest security return (Agustini et al. 2021). Emerging threats, including cyber-attacks and insider threats, are also highlighted as areas requiring further investigation and coordinated responses. Within this forward-looking agenda, advanced tools such as biometrics, artificial intelligence, and predictive analytics are frequently discussed as potential avenues for improving detection and efficiency, alongside continued attention to governance and ethical alignment (Klenka 2019; Sakano et al., 2016).

Deterrence theory and aviation security effectiveness

This study adopts deterrence theory as a supporting analytical lens for interpreting how aviation security measures may influence the likelihood of unlawful interference. Deterrence theory, rooted in criminology, proposes that the anticipation of punishment and other adverse consequences can discourage unlawful behavior when deterrent threats are credible and perceived as enforceable (Tomlinson 2016). In its classical formulation, deterrence assumes that offenders often behave as rational decision-makers who weigh expected benefits against expected costs. When perceived costs, particularly detection, arrest, and punishment, exceed anticipated gains, individuals are expected to refrain from unlawful behavior (Nagin 2013).

The intellectual foundations of deterrence theory are commonly traced to classical criminological and political philosophy, including the writings of Thomas Hobbes, Cesare Beccaria, and Jeremy Bentham. Beccaria's contribution is especially relevant for deterrence-based security reasoning, as it emphasizes rational self-interest and the expectation that individuals avoid criminal acts when costs outweigh benefits (Beccaria, 1963). Within this framework, severity of punishment may contribute to deterrence, but sustained deterrent effects depend primarily on the credibility of enforcement and the belief that consequences will occur.

Applied to aviation security, deterrence theory offers a structured approach for understanding how security measures shape offender perceptions. Practices such as screening, surveillance, access control, and rapid response mechanisms may deter unlawful interference when they increase the perceived likelihood of detection and convey that serious consequences will follow attempted breaches. This perspective aligns with arguments that deterrence-based effectiveness depends on perceptions regarding the capacity and willingness of authorities to impose meaningful consequences (Jackson et al. 2012; Zilincik and Sweijs 2023). In practical terms, the vis-

ibility of security personnel, the presence of sophisticated screening procedures, and the deployment of technological surveillance systems can elevate perceived risks for potential offenders, thereby discouraging aviation crimes (Baker 2020).

Deterrence theory, however, requires careful application in complex security environments. Empirical demonstration of deterrence is challenging when offenders adapt behavior, when threats shift across domains, or when attackers adjust tactics in response to security measures (Jackson et al. 2007; Nagin 2013). Aviation security provides a particularly relevant illustration of these challenges, as adversaries may adapt their strategies, circumvent existing controls, and exploit emerging vulnerabilities as protective systems evolve. Despite these limitations, deterrence theory remains analytically useful as a heuristic framework for organizing how perceived risks and security measures may be related (Jackson et al., 2012).

Consistent with this perspective, deterrence in aviation security is not limited to punishment threats but is also produced through layered systems that signal detection capability. Screening procedures, explosive detection technologies, risk-based profiling, and intelligence-informed threat assessment can function as deterrence mechanisms insofar as they increase perceived difficulty and reduce expectations of successful interference (Klenka 2019). Deterrence dynamics may also vary across actor types, as motivations and strategic calculations differ between individuals and organized groups, making this distinction relevant when evaluating deterrent capacity (Klenka 2019; Morral et al., 2014). Cyber threats further extend deterrence considerations beyond physical screening contexts, as attacks targeting critical aviation systems require adaptation of deterrence logic to digital domains (Agustini et al. 2021).

In this study, deterrence theory is used to structure the interpretation of aviation security practices and narratives, with particular attention to perceived detection risk, credible consequences, and system-level conditions that may enable or constrain deterrence. Within this framing, aviation security is approached as an evolving and context-dependent environment rather than a system in which deterrence effects can be directly inferred or measured. This perspective also aligns with policy and practice discussions emphasizing evidence-based evaluation and cost-effectiveness of security programs, particularly in contexts where technologies are financially demanding, operationally complex, or influential in shaping passenger experience (Jackson et al. 2012; Merhi and Ahluwalia 2019; Stewart and Mueller 2011).

Methodology

This study adopts a qualitative research approach to examine the effectiveness of aviation security measures and to explore how these measures are interpreted, implemented, and experienced by aviation security professionals within operational settings. Qualitative inquiry is appropriate for this purpose because it enables an in-depth understanding of professional experience, operational judgment, and organizational context, dimensions that are not readily captured through standardized measurement. Given the complexity of aviation security and the restricted accessibility of many operational environments, a qualitative design also provides opportunities to examine forms of experiential and practice-based knowledge that are difficult to observe

through quantitative approaches alone. Accordingly, the methodological design is intended to generate contextually grounded insights into how practitioners understand security effectiveness, deterrence, implementation challenges, and evolving threats within contemporary civil aviation.

The study draws on practitioner narratives as its primary qualitative data source, with storytelling used as a methodological orientation to facilitate the elicitation of experience-based accounts of everyday aviation security practice. This includes how professionals interpret threats, manage operational constraints, and assess security effectiveness in real settings (Maitlis and Lawrence 2007). Rather than being treated as literary artefacts, practitioner narratives are regarded as empirical accounts through which professionals interpret operational realities, negotiate uncertainty, and make sense of security practice (Hyvärinen 2008). Storytelling therefore serves as a means of eliciting qualitative data, while thematic analysis provides the analytical procedure through which patterns and meanings are identified and interpreted.

Research design

The study employs a qualitative research design to examine how aviation security professionals understand and evaluate security measures within the context of unlawful interference. Particular attention is given to operational challenges, critical incidents, perceived effectiveness, and the evolving nature of contemporary security practice. This design enables examination of how aviation security professionals interpret, implement, and evaluate security practices in real operational settings. Semi-structured interviews were selected as the primary data collection method to support systematic, yet flexible exploration of professional experience related to aviation security and deterrence.

Qualitative research is well suited to addressing how and why questions that arise in complex institutional environments, where practices and judgments are shaped by context and experience rather than by variables that can be readily quantified (Cleland 2017). Within aviation security, effectiveness cannot be understood solely through formal procedures or technical specifications; it also depends on how security measures are interpreted, adapted, and enacted by those responsible for their implementation.

The study is informed by a constructivist research philosophy, which assumes that social reality is shaped through interaction, interpretation, and experience (Pilarska 2021). Assessing the effectiveness of aviation security measures therefore requires examination of the perspectives and experiences of professionals who design, implement, or oversee these measures. Prior research emphasizes that security practices are best understood through the viewpoints of those directly involved in or affected by them, as these perspectives reveal how formal rules operate in practice and where gaps or tensions may emerge (Singh and Singh 2003).

This constructivist positioning allows close attention to the practical use of security measures and to variations in how similar procedures produce different outcomes across contexts. Rather than aiming for statistical generalization, the study seeks to generate theoretically informed and practice relevant understanding of how aviation security operates under specific institutional and regulatory conditions. Consistent

with this methodological orientation, semi-structured interviews were designed to encourage participants to recount incidents, routine practices, dilemmas, and evaluations arising from their professional experience. These narratives subsequently formed the empirical material for thematic analysis rather than constituting a distinct analytical approach in themselves (Hadi and Closs 2015).

Data collection

Data were collected through semi-structured, in-depth interviews with aviation security professionals. This approach is well suited to examining complex professional practices and decision making in contexts where formal procedures interact with experience-based judgment (Wilson 2015). In depth interviews enable systematic exploration of meanings, interpretations, and evaluative assessments that are not readily captured through standardized instruments.

The data collection process involved careful preparation, including review of relevant academic research and policy frameworks to inform the development of the interview guide (Deterding and Waters 2018). Interviews followed a semi-structured format to ensure analytical consistency across participants while allowing flexibility to pursue issues that emerged during the conversation (Karatsareas 2022; Osborne & Grant Smith, 2021n). This format supported the qualitative design of the study by allowing participants to articulate experiences, incidents, and professional judgments in their own terms.

The interview guide was organized around the core research aims and included predefined thematic prompts addressing the effectiveness of aviation security measures in preventing unlawful interference, cross border collaboration and intelligence sharing practices, and awareness and communication related to passenger and airport security. Interviews typically began with general, experience focused questions before progressing to more specific or sensitive topics, in line with established qualitative interviewing guidance (Roulston 2017). Open ended follow up questions were used throughout to encourage elaboration, clarification, and reflection on practical implications.

Data collection was conducted entirely online to accommodate professional responsibilities and geographical dispersion among participants. Three interviews were conducted synchronously using Zoom and were audio recorded with participants' informed consent. One participant, due to time constraints, provided written responses to the interview questions through an asynchronous online format. Interview duration for synchronous sessions was approximately one hour, although length varied depending on availability and depth of discussion.

All audio recorded interviews were transcribed verbatim shortly after completion to preserve contextual detail and analytic accuracy. Interview questions were shared with participants in advance to allow time for reflection and clarification where appropriate. The complete interview guide, including indicative questions, is provided in Appendix A.

Participant selection and profile

Participants were selected using purposive sampling, a strategy commonly employed in qualitative research to identify individuals with direct experience and substantive knowledge of the phenomenon under investigation (Creswell 2009; Robinson 2013). Selection focused on aviation professionals with extensive operational or regulatory involvement in aviation safety, security, and risk management, as such experience is essential for examining the effectiveness and practical implementation of aviation security measures.

The final sample consisted of four aviation professionals, each with a minimum of eight years of professional experience in the aviation sector. All participants were actively engaged in roles related to aviation security, safety oversight, or organizational risk management at the time of data collection. To reflect the international and regulatory diversity inherent in aviation security practice, participants were drawn from Europe and Africa, while maintaining a shared analytical focus on internationally recognized aviation security standards, particularly ICAO Annex 17. An overview of participant characteristics, including professional roles, organizational affiliations, regional context, and interview modes, is presented in Table 1.

Participants were assigned anonymous numerical identifiers, which are used consistently throughout the Findings section to attribute quotations. The combination of airline based operational roles, regulatory oversight functions, and aviation safety

Table 1 Characteristics of interview participants

Participant	Primary role	Organizational affiliation	Functional area	Region	Interview mode	Interview duration	Experience
Anonymous 1	AVSEC risk and threat analyst	National airline (international airport operations)	Aviation security and threat analysis	Africa (Kigali)	Online synchronous interview (Zoom)	Approximately 60 min	15 years
Anonymous 2	Safety and security expert and lecturer	Aviation manufacturer and training context (Airbus)	Safety management and crisis management	Europe (France)	Written qualitative responses	Not applicable	22 years
Anonymous 3	Airworthiness expert and aviation safety advocate	National civil aviation authority	Regulatory oversight and compliance	Africa (Kenya)	Online synchronous interview (Zoom)	Approximately 50–55 min	18 years
Anonymous 4	Safety risk manager	National airline	Organizational risk management	Africa (Kigali)	Online synchronous interview (Zoom, two sessions)	Approximately 30–35 min per session	12 years

and training expertise enabled the study to capture complementary perspectives on aviation security practice, risk management, and regulatory governance, while preserving analytical coherence across participants.

Research rigor and trustworthiness

Ensuring rigor in qualitative research requires approaches that differ from those typically applied in quantitative designs. Rather than relying on measurement consistency or statistical inference, qualitative inquiry establishes rigor through criteria that support trustworthiness, interpretive coherence, and analytical transparency (Lincoln and Guba 1985). In this study, rigor was addressed through credibility, dependability, reflexivity, and ethically responsible research practice, consistent with interpretive and narrative research designs.

Credibility was supported through triangulation, which involved comparing insights across participants and thematic patterns rather than relying on single accounts (Denzin 2012). Analytical emphasis was placed on identifying convergent and divergent interpretations across narrated experiences. Sustained engagement with the research topic and repeated interaction with participants further contributed to contextual understanding and interpretive depth.

Dependability and transparency were addressed through thick description and systematic documentation of the research process. Detailed contextual information was provided regarding the study setting, participant characteristics, data collection procedures, and analytic decisions, enabling readers to assess the plausibility and transferability of the findings within comparable institutional or regulatory environments (Geertz 1973). An audit trail was maintained throughout the study, documenting methodological choices, coding decisions, and the development of themes, thereby allowing external assessment of how interpretations were derived from the data (Miles et al. 2014).

Peer debriefing enhanced analytical clarity through iterative discussions of emerging interpretations and thematic structures with fellow researchers. Member checking was applied selectively by sharing synthesized interpretations with participants to confirm resonance with their professional experience while preserving analytical independence.

Given the qualitative design of the study and its use of practitioner narratives as data, reflexivity was treated as a core element of rigor. The researcher maintained field notes documenting positionality, prior assumptions, and potential influences on interpretation. Narrative excerpts were selected with care to preserve professional voice and avoid decontextualization. Anonymization procedures ensured that quotations functioned as illustrative evidence rather than identifiable accounts.

Ethical considerations were embedded within these rigor-oriented practices. All research activities were conducted in accordance with relevant ethical guidelines and regulations governing research involving human participants, and formal ethics approval was obtained prior to data collection. Ethical guidance issued by professional bodies, including the British Educational Research Association (2011) and the American Educational Research Association (2011), informed the conduct of the study alongside applicable institutional and national regulations. Participation was

voluntary, informed consent was obtained prior to involvement, confidentiality was safeguarded through pseudonyms and de-identification, and access to research materials was restricted to the research team.

Data analysis

Data analysis followed a qualitative thematic approach consistent with the interpretive and storytelling-oriented design of the study. Thematic analysis was selected because it provides a systematic yet flexible framework for identifying, analyzing, and interpreting recurring patterns within qualitative data (Braun and Clarke 2006). This approach is well suited to examining meaning, experience, and evaluation across narrated accounts and is adaptable across theoretical perspectives and applied research contexts (Kiger and Varpio 2020).

The analytic process involved close engagement with interview transcripts to identify initial codes capturing recurring ideas, practices, and concerns related to aviation security effectiveness, deterrence, collaboration, and awareness. Coding focused on both explicit content and underlying evaluative judgments expressed in participants' narratives. Codes were then examined for conceptual similarity and organized into broader themes that reflected shared patterns across accounts while remaining sensitive to contextual variation.

Analysis was iterative and interpretive rather than linear. Themes were refined through repeated comparison across transcripts, with attention to convergence and divergence in how participants described security practices, perceived threats, and operational challenges. Qualitative data management software was used to support systematic coding and organization of the dataset.

Although participants shared their experiences in narrative form, the study does not adopt narrative analysis as its methodological framework. Instead, these accounts are treated as qualitative empirical material and analyzed using thematic analysis to identify patterns of meaning across participants' experiences. Storytelling therefore serves to elicit rich experiential accounts, whereas thematic analysis provides the analytical procedure through which these accounts are interpreted. Findings are presented through carefully selected quotations that illustrate the analytical interpretations while enhancing transparency. Pseudonyms are used throughout to protect participant confidentiality and preserve continuity across the reported accounts.

Findings

This section presents the empirical findings derived from in-depth interviews with aviation security professionals. In keeping with a storytelling-informed qualitative approach, participants' quotations are used as contextualized narrative evidence illustrating how security effectiveness, constraints, and improvement needs are experienced and interpreted in practice. Rather than being treated as isolated statements, quotations are presented as situated accounts that reflect how practitioners make sense of aviation security within operational settings.

The findings are organized around six overarching themes that correspond directly to the analytical structure summarized in Table 2. These themes emerged through iterative thematic analysis and capture shared patterns across the dataset while retaining sensitivity to contextual variation. To complement the thematic presentation, Appendix B presents four integrated case summaries based on participant accounts, illustrating how multiple themes intersect within concrete professional experiences. Figure 1 provides a visual overview of the relative salience of the six themes across the four vignettes and is intended as an interpretive aid rather than an indicator of relative importance.

Balancing security and privacy

Participants consistently described aviation security as an operational domain shaped by an ongoing tension between security imperatives and privacy considerations. Rather than approaching privacy as an abstract ethical concern, participants emphasized how privacy obligations directly influence the design, scope, and application of screening practices, operational procedures, and regulatory adaptations in everyday airport operations.

Privacy was frequently discussed as a practical constraint on the uniform application of security measures, particularly during passenger screening. Cultural norms, legal differences, and levels of public acceptance were described as shaping how screening procedures are implemented across contexts. As one participant stated, "*To some extent privacy may hinder the proper application of security measures like screening at checkpoints due to different factors like culture*, *special procedures and operational deficiencies*" (Anonymous 1). These constraints were seen as especially salient in international travel settings, where security personnel must navigate overlapping and sometimes conflicting regulatory expectations.

Participants emphasized that effective aviation security depends on maintaining legitimacy and public trust. Screening practices were described as sustainable only when they are perceived as proportionate, transparent, and consistently applied. This view is reflected in the observation that "*striking a balance between ensuring passenger safety and respecting privacy rights is essential*, *and security measures should remain proportionate and transparent*" (Anonymous 4). From this perspective, privacy considerations were not framed as obstacles to security, but as conditions that shape how security measures are accepted and upheld in practice.

Collaboration and coordination

Aviation security was uniformly portrayed as a collective and transnational responsibility, dependent on coordination among multiple actors operating across organizational and national boundaries. Participants emphasized that no single authority could manage aviation security in isolation, given the interconnected nature of air transport systems.

Trust and confidentiality emerged as foundational elements of effective collaboration, particularly in relation to intelligence exchange. Participants stressed that timely sharing of sensitive information requires confidence in counterpart institutions and clear protocols governing information use. As one participant noted, "*Building trust and confidentiality around security matters is essential for effective cooperation*"

Table 2 Themes, subthemes, illustrative codes, and frequencies

Theme	Subtheme	Illustrative codes	Frequency
Balancing security and privacy	Privacy–security trade-off	Balancing privacy and security in aviation screening	2
		Harmony and regulatory adaptation in aviation privacy	1
	Screening practices	Checks and searches	2
		Screening of passengers	3
	Operational procedures	Procedures	2
Collaboration and coordination	Trust and confidentiality	Building confidentiality	1
		Regular contacting with agencies	1
	Intelligence exchange	Intelligence collaboration	2
	Training and awareness	Personnel training and security awareness	2
	Standards and compliance	Security standards	1
Human factors and training	Definitions of unlawful interference	Jeopardizing the safety of civil aviation	3
		Airborne hostage situations	1
		Aircraft seizure	1
		Aircraft destruction	1
	Personnel training	Role-based security training	1
		Safeguard standard procedures	1
	Security culture	Security culture	1
	Professional experience	Participants' experience in aviation	3
Security measures and effectiveness	Innovation and emerging risks	Emerging technologies and sustainable innovations	2
		Emerging threats to civil aviation	1
		Unidentified aircraft	1
	Proactive risk management	Strategic approaches to risk assessment	2
		Innovative security technologies	1
	Effectiveness outcomes	Adaptability and flexibility	1
		Building public confidence	1
		Passenger awareness	1
	Implementation challenges	Inability to comply	2
		Poor standards and regulations	1
		Training of personnel	1
		High budget constraints	1
	Evolution of measures	Documentation and implementation	1
		Monitoring processes	3
Technology and procedures	Technological impact	Technology advancement impact on aviation security	3
		Balancing positive and negative effects of technology	1
Threat landscape and mitigation	Understanding threat environment	Adapting to evolving threats	1
		Monitoring challenges in airport operations	1
		Complexity of airport operations and stakeholders	1

Table 2 (continued)

Theme	Subtheme	Illustrative codes	Frequency
	Insider threat awareness	Sharing of sensitive information	2
		Smuggling into restricted areas	2
		Vulnerability	1
	Response strategies	Cybersecurity and AI	3
		Integration and advancement of security systems	1
		Preventive measures against threatening items	2
	Regulatory oversight	Regulatory framework	2

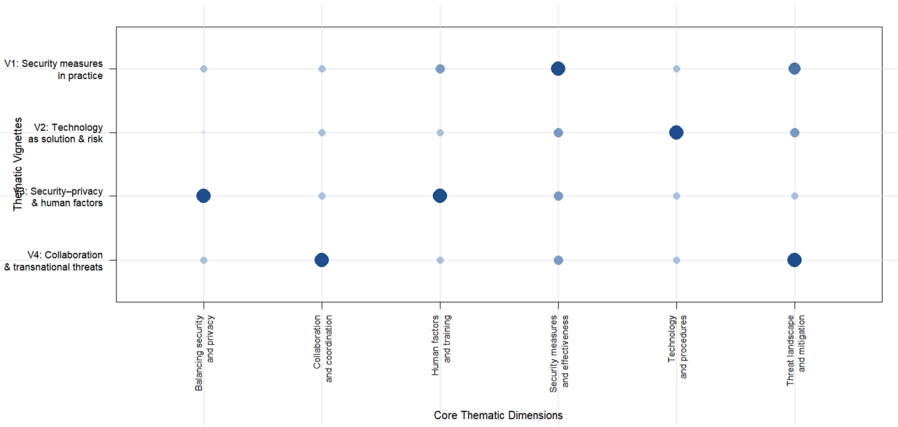

Fig. 1 Thematic salience across aviation security vignettes

(Anonymous 3). Intelligence exchange was described as an ongoing and institutionalized process rather than an episodic response to specific incidents.

Training and shared standards were also identified as critical enablers of coordination. Participants highlighted the role of international aviation security frameworks in aligning practices across jurisdictions, while acknowledging uneven implementation and compliance. Regular interaction with international partners, joint training initiatives, and continuous engagement with regulatory bodies were described as mechanisms through which coordination is sustained over time.

Human factors and training

Human factors emerged as a central pillar of aviation security, encompassing professional experience, shared understandings of unlawful interference, and organizational security culture. Participants consistently emphasized that effective security relies not only on systems and procedures, but also on the judgment, awareness, and experience of personnel.

Participants demonstrated a shared conceptualization of unlawful interference as acts that threaten the safety of civil aviation, including aircraft seizure, hostage-tak-

ing, and the destruction of aircraft. These understandings were grounded primarily in professional practice and historical incidents rather than in formal legal definitions. This perspective is reflected in the view that "*unlawful interference fundamentally means any act that jeopardizes the safety of civil aviation*" (Anonymous 2).

Training and experience were repeatedly identified as critical for translating formal procedures into effective action. Role-based security training, continuous professional development, and reinforcement of security culture were described as essential for detecting weak signals and responding to evolving threats. As one participant emphasized, "*Nothing can replace human intelligence and the weak signals that experienced personnel can detect*" (Anonymous 3). Participants stressed that technology could support decision-making but cannot substitute for professional judgment embedded in experience.

Security measures and effectiveness

Participants conceptualized aviation security effectiveness as dynamic and contingent, shaped by innovation, risk management practices, and implementation capacity. Security was not viewed as a fixed set of controls, but as an evolving system that must adapt continuously to emerging risks.

Innovation and proactive risk management were described as necessary responses to changing threat profiles, including emerging technologies and new forms of unlawful interference. Participants emphasized that innovation should be embedded within broader security strategies rather than introduced as isolated technical fixes. This orientation is captured in the view that "*security measures must evolve continuously to address emerging threats to civil aviation*" (Anonymous 4).

At the same time, participants highlighted persistent implementation challenges. Effectiveness was associated with adaptability, flexibility, public confidence, and passenger awareness, but constrained by gaps in compliance, insufficient training, regulatory inconsistencies, and limited resources. As one participant explained, "*Security measures are effective only if they are properly documented*, *implemented*, *and monitored by all stakeholders*" (Anonymous 1). From this perspective, effectiveness depended as much on governance and coordination as on technical capability.

Technology and procedures

Technology was described as both an enabler of aviation security and a source of new operational and ethical complexities. Participants widely acknowledged that technological advancements have improved detection capabilities, processing efficiency, and situational awareness.

Participants cautioned against over-reliance on automated systems and emphasized the importance of anticipating unintended consequences associated with technological deployment. The dual nature of technological change was reflected in the observation that "*technology has started to impact security measures in both positive and negative ways*, *and the aviation community must be prepared for both*" (Anonymous 1). These concerns extended to potential system failures, ethical implications, and the gradual erosion of human oversight.

Participants emphasized that technological innovation must be balanced with regulatory guidance, professional judgment, and public acceptance. In particular, AI-driven and biometric systems were described as effective only when embedded within clear governance frameworks and supported by trained personnel capable of interpreting outputs critically.

Threat landscape and mitigation

The final theme captured participants' perceptions of an increasingly complex and evolving threat environment facing aviation. Participants described contemporary threats as multifaceted, encompassing operational vulnerabilities, insider threats, geopolitical instability, and cyber-related risks.

Insider threats were repeatedly emphasized as a critical concern, particularly in large and complex airport environments where continuous monitoring is challenging. As one participant observed, "*If there is a way to cause damage or extract gain*, *there is always a vulnerability to insider threats*" (Anonymous 2). Such vulnerabilities were linked to shortcomings in background checks, organizational oversight, and security culture.

Mitigation strategies were described as requiring a combination of technological safeguards, preventive screening measures, and robust regulatory oversight. Participants stressed that cybersecurity, AI-enabled monitoring systems, and coordinated regulatory enforcement play an increasingly important role in addressing emerging threats. Overall, the findings portray aviation security as a socio-technical system in which effectiveness depends on the interaction of human expertise, technological capability, organizational coordination, and adaptive governance.

Discussion and implications

The findings suggest that the effectiveness of contemporary aviation security cannot be understood solely through technical safeguards or formal regulatory compliance mechanisms (Pettersen and Bjørnskau 2015). Rather, security emerges through the interaction of professional judgment, organizational routines, institutional coordination, and layered deterrence practices operating within complex operational environments. Participants' accounts indicate that deterrence is experienced not merely through the existence of formal sanctions, but through the visible presence of security measures, uncertainty, and perceptions concerning the likelihood of detection and intervention (Kirschenbaum et al. 2012).

In line with core assumptions of deterrence theory, participants described visible and stringent security measures such as biometric screening, layered access control, and surveillance systems as influential in shaping offender behavior by increasing perceived risks associated with unlawful interference (Cornish and Clarke 2016; Hodwitz 2020). These observations suggest that deterrence within aviation environments operates not only through punitive consequences, but also through visible surveillance capability, procedural unpredictability, and institutional preparedness. This interpretation aligns with prior research portraying offenders as actors who assess potential gains against anticipated costs and consequences. At the same time, the

findings suggest that the preventive capacity of security measures varies across threat categories and operational settings, particularly where organizational familiarity and privileged access reduce the effectiveness of conventional control systems.

A particularly salient issue concerns insider threats. Unlike external adversaries, insiders operate with procedural familiarity, contextual knowledge, and privileged access, conditions that may weaken the perceived reach of conventional preventive controls. Participants' accounts illustrate how routine practices, organizational blind spots, or diminished vigilance can enable unlawful acts, whether through deliberate misconduct or inadvertent error. Consistent with earlier aviation-security research emphasizing the persistence of insider vulnerabilities within highly regulated transport environments (Loffi and Wallace 2014; Willison et al. 2018), the findings suggest that security failures may emerge not only from external intrusion but also from the internal dynamics of organizational systems themselves. This pattern complicates deterrence models grounded solely in rational choice assumptions and highlights vulnerabilities that originate within organizational systems rather than external attack vectors alone (Willison et al. 2018).

Viewed collectively, these findings reflect broader post-9/11 transformations in aviation security governance, where effective protection increasingly depends on adaptive coordination among technological systems, institutional oversight, and human interpretation rather than on static procedural compliance alone. The capacity of protective systems to function effectively therefore appears contingent on how responsibilities are interpreted, enacted, and sustained across organizational levels. From this perspective, aviation security functions as a socio-technical and continuously adaptive system in which deterrence, operational practice, and organizational culture remain deeply interconnected.

Theoretical implications

This study advances deterrence theory by moving beyond a static and offender-centered interpretation and situating deterrence within the organizational and experiential contexts in which aviation security is enacted. Classical deterrence theory is grounded in the assumption that individuals assess the expected costs and benefits of unlawful behavior in a largely rational manner (Cornish and Clarke 2016). The findings indicate that such assessments, as understood by practitioners, are shaped by institutional position, access privileges, and perceptions of visibility within security systems. Accordingly, deterrence does not operate uniformly across actor categories, particularly in environments where insider access alters perceptions of surveillance, accountability, and sanction. Insider threats therefore reveal important limitations in conventional deterrence assumptions.

Insiders' familiarity with procedures, routines, and enforcement practices alters how risk and sanction are perceived, reducing the effectiveness of deterrence mechanisms that rely primarily on detection and punishment. This finding challenges the implicit universality often associated with deterrence theory and suggests that deterrent processes must be interpreted in relation to organizational embeddedness, operational proximity, and role-specific perceptions within complex socio-technical environments such as civil aviation. Rather than functioning as a uniform behavioral response, deterrence appears as a contingent process shaped by proximity to control systems and everyday organizational practice.

Methodologically, the use of storytelling as an analytical lens contributes to theoretical development by revealing how deterrence is interpreted, enacted, and sometimes bypassed in practice. Narratives provided by aviation security professionals do not merely report compliance or non-compliance; they reflect how actors make sense of risk, responsibility, and effectiveness within constrained operational environments. From this perspective, narratives function not simply as descriptive accounts, but as interpretive spaces through which security practices, institutional expectations, and deterrent logics are continuously negotiated and re-evaluated (van Hulst and Tsoukas 2023). This perspective supports the view that security is not simply imposed through formal regulation but is actively constructed through professional judgment and organizational interaction (Salter 2008).

The findings also reinforce the need to integrate deterrence theory with human factors and security culture perspectives. Deterrence emerges as inseparable from awareness, motivation, and shared norms that govern how security measures are implemented and sustained. Technological controls and formal sanctions provide necessary conditions for deterrence, but they are insufficient in the absence of organizational cultures that reinforce accountability, vigilance, and responsibility. Viewed in this way, deterrence is better understood as an adaptive socio-technical process shaped through the ongoing interaction of institutional practices, behavioral expectations, and technological systems rather than as an isolated punitive mechanism detached from operational context.

The study contributes theoretically by framing deterrence as an organizationally embedded and experience-driven process shaped by roles, sensemaking practices, and security culture. This perspective extends beyond aviation settings and offers broader relevance for other high-reliability sectors characterized by complexity, interdependence, and evolving risk conditions, where formal controls remain closely intertwined with human judgment and organizational coordination.

Moreover, as the aviation sector approaches the twenty-fifth anniversary of the September 11 attacks, the findings highlight how contemporary aviation security increasingly depends on organizational vigilance, operational coordination, and human judgment alongside surveillance and procedural control. Participants' narratives suggest that current security vulnerabilities may emerge through routine practices and organizational processes as much as through external threats. This observation aligns with broader post-9/11 discussions advocating more adaptive, intelligence-informed, and human-centered approaches to aviation security governance capable of responding to evolving threat environments and organizational complexity (Komasová 2020; Salter 2008).

Managerial and policy implications

The findings point to several implications for aviation security managers responsible for operational design and resource deployment. One recurring managerial lesson concerns the role of visibility and unpredictability in sustaining deterrence. Security practices that rely on fixed routines and highly standardized procedures were described by participants as increasingly vulnerable to anticipation and exploitation. In contrast, randomized screening protocols, irregular patrol patterns, and non-routine

checks were viewed as effective in disrupting both external offenders' planning and insiders' ability to exploit procedural familiarity. Such practices increase uncertainty, reduce procedural predictability, and reinforce deterrence without necessarily requiring continual escalation of coercive security measures (Hicks 2016; Pita et al. 2009).

Resource allocation decisions also carry important implications. While permanent deployment of armed personnel and manual inspections enhances perceived security presence, these measures impose significant financial and human resource costs. The findings suggest that advanced screening technologies, including biometric systems and automated detection tools, can support deterrence objectives while improving operational efficiency (Nikolaev et al. 2012). However, technological systems are most effective when they complement, rather than replace, human judgment. Managerial attention is therefore required to ensure that technological investments are accompanied by training, oversight, and clear decision protocols that preserve professional discretion.

Security culture emerged as a central managerial lever for reducing vulnerability, particularly in relation to insider threats. Regular training, role-specific risk assessments, and structured incident reporting mechanisms were described as essential for sustaining vigilance and shared responsibility. Rather than functioning as isolated interventions, these practices shape how personnel interpret and enact security requirements in everyday operations. From a managerial perspective, cultivating security culture involves sustained engagement with staff, reinforcement of accountability norms, and organizational support for reporting concerns without fear of reprisal (Low and Yang 2019).

At the policy level, the findings draw attention to the ongoing challenge of balancing enhanced security capabilities with the protection of passenger privacy. Technologies such as facial recognition, full-body scanners, and passenger profiling expand detection capacity but raise legal and ethical questions related to data protection and bodily integrity (Bryan 2018; Nugraha and Choi 2016). Participants' accounts indicate that public acceptance of these measures depends less on their technical sophistication than on perceptions of proportionality, transparency, and procedural fairness.

In this context, privacy-by-design principles offer a practical policy pathway for integrating security and rights protection. Embedding privacy safeguards into the early stages of system design and implementation enables authorities to pursue deterrence objectives while maintaining public trust and regulatory legitimacy (Cavoukian and Jonas 2012). Participants' narratives further suggest that transparent communication regarding data use, retention practices, and accountability procedures remains essential for sustaining confidence in aviation-security institutions.

The findings further emphasize the importance of international coordination in aviation security governance. Given the transnational nature of air transport, uneven implementation of security standards across jurisdictions creates structural vulnerabilities that can be exploited by both external and insider actors. International frameworks such as ICAO Annex 17 and associated audit mechanisms play a key role in promoting alignment and mutual accountability (ICAO, 2017). Consistent with broader post-9/11 aviation-security governance discussions, the study highlights the continuing importance of intelligence sharing, regulatory cooperation, and trust-based institutional coordination among states in supporting collective security resilience (Salter 2008).

Limitations and future research directions

This study has several limitations that should be considered when interpreting the findings. The analysis draws on in-depth narratives provided by a small group of aviation security professionals. This design reflects the qualitative and storytelling-informed orientation of the study, privileging depth of understanding over breadth of coverage. The final sample consisted of four participants, one of whom provided written responses rather than participating in a synchronous interview. Although this approach enabled the inclusion of a professionally experienced participant whose scheduling constraints limited availability, differences in data collection format may have influenced the level of detail, interaction, and spontaneity reflected in the data. Given the limited sample size, the findings should be interpreted as exploratory and context specific rather than representative of the broader aviation sector. The findings therefore offer analytically grounded interpretations of how deterrence and security practices are understood and enacted in professional contexts, rather than claims of statistical generalizability. Moreover, the findings reflect participants' professional interpretations of aviation security effectiveness rather than objective evaluations of the performance of specific security measures. They should therefore be understood as informed practitioner perspectives on aviation security rather than direct assessments of operational effectiveness. Variations in regulatory regimes, organizational arrangements, and resource conditions across regions may shape aviation security practices in ways that are not fully represented in this dataset.

Research access constraints inherent to security-sensitive domains also shaped the scope of empirical material. Professional confidentiality obligations and ethical considerations limited the discussion of certain operational details, particularly those related to classified procedures, intelligence-sharing arrangements, and covert deterrence strategies. Although such constraints are common within aviation-security research, they may have restricted insight into informal routines, tacit coordination processes, and discretionary practices operating alongside formal institutional controls.

The study relies on self-reported professional accounts, which reflect participants' interpretations and experiences rather than direct observation of security operations. Such narratives are well suited to examining sensemaking, judgment, and organizational culture, but they may also be influenced by institutional positioning, professional norms, and retrospective framing. Additional methodological approaches, including ethnographic observation, document analysis, or scenario-based simulations, could provide complementary insight into how protective practices are enacted under real-time operational conditions, while enabling comparison between practitioner perceptions and observed organizational practices.

These limitations suggest several avenues for future research. Comparative studies across different regulatory and institutional contexts would help clarify how deterrence mechanisms and security cultures vary between regions, airport types, and governance arrangements. Longitudinal research designs could further illuminate how deterrence practices and threat perceptions evolve over time in response to technological innovation, major security incidents, or regulatory change.

Further work could also integrate qualitative insights with quantitative or mixed-method approaches to examine links between perceived deterrence, security behav-

ior, and measurable outcomes. More focused examination of insider-threat dynamics, particularly in relation to organizational trust, reporting practices, and accountability structures, would contribute to a deeper understanding of vulnerabilities that remain difficult to address through conventional deterrence approaches alone.

Emerging challenges associated with cyber-enabled threats, unmanned aircraft systems, and AI-driven security technologies also warrant sustained scholarly attention. As aviation security systems become more digitally integrated, future research should examine how deterrence operates in hybrid human–machine environments and how responsibility, oversight, and professional judgment are reconfigured within increasingly automated security architectures.

Conclusion

This study examined how aviation security effectiveness is understood and enacted in practice by professionals directly responsible for its implementation. The findings showed that aviation security could not be reduced to technical safeguards or formal regulatory compliance alone. Instead, security emerged through the interaction of deterrence practices, professional judgment, organizational routines, and regulatory coordination within complex operational environments.

Practitioners' experiential accounts illustrated how deterrence operated through visibility, uncertainty, and routine enforcement activity while simultaneously revealing structural limitations associated with insider threats and organizational embeddedness. The analysis further showed that operational outcomes depended not only on the existence of formal controls, but also on how responsibilities, procedures, and institutional expectations were interpreted, sustained, and adapted by human actors working within constrained organizational settings.

The study also demonstrated that technological advancement, while central to contemporary aviation governance, reshaped rather than resolved existing challenges. Emerging systems introduced additional ethical, oversight, and accountability considerations that required continual adjustment of professional roles, institutional responsibilities, and operational capabilities. Protective capacity therefore appeared to depend less on isolated technological interventions than on evolving combinations of human expertise, technological support, and cooperative governance structures.

Methodologically, the storytelling-informed qualitative approach adopted in this study provided access to dimensions of aviation practice that remain difficult to capture through conventional evaluative metrics. Treating professional narratives as sites of sensemaking rather than merely illustrative examples enabled a practice-oriented perspective that complemented predominantly technical and policy-centered approaches within existing aviation-security scholarship.

Although the complete elimination of risk within civil aviation remains unattainable, the findings suggest that more resilient protective arrangements are those capable of learning, adaptation, and reflexive governance. Approaches attentive to human factors, institutional context, and evolving threat conditions offer a more sustainable basis for addressing unlawful interference within increasingly interconnected and technologically mediated aviation environments.

Appendix A

Table 3 Interview questions

1. How would you describe your professional background and experience within the aviation industry?
2. Based on your professional experience, how would you assess the current effectiveness of aviation security measures in mitigating potential threats?
3. How do you conceptualize unlawful interference within the context of aviation security?
4. In your view, which security measures play the most critical role in safeguarding aviation operations against unlawful acts?
5. Can you reflect on any incidents or events that, in your experience, illustrate the importance of security measures in preventing unlawful acts?
6. From your perspective, what are the main strengths and limitations of existing security measures in the aviation industry?
7. How has the aviation industry adapted its security practices in response to emerging threats associated with unlawful interference?
8. What key challenges do aviation professionals encounter in the implementation and maintenance of effective security measures?
9. To what extent do you think emerging technologies, such as biometric identification or artificial intelligence, are influencing aviation security procedures?
10. Are there particular areas within aviation security research that you consider underexplored or in need of further investigation?
11. What types of security training and operational protocols are currently in place to support airport personnel in identifying and responding to potential security threats?
12. In your opinion, what insider threat risks should airport authorities be particularly attentive to?
13. From your perspective, what factors or motivations tend to underline unlawful activities occurring within airport environments?
14. To what extent are security audits and risk assessments routinely conducted to identify potential vulnerabilities?
15. How do you perceive the balance between passenger privacy rights and safety requirements during security screening and checkpoint procedures?
16. What approaches or strategies have you found to be effective in adapting to evolving unlawful threats?
17. How do aviation authorities contribute to the prevention of security threats, and are there specific traveler behaviors that may signal elevated risk?
18. Looking ahead, how do you anticipate innovations in aviation, such as unmanned aircraft systems, may influence the nature or intensity of future security threats?

Appendix B

Table 4 Thematic vignettes

Vignette 1. Security measures and effectiveness in practice
One participant characterized aviation security as a layered system shaped by experience rather than design alone. Drawing on extensive involvement in airline operations and safety management, airport security was described as operating within environments that are inherently open, complex, and difficult to enclose. Large airport infrastructures were portrayed as spaces where accessibility is unavoidable and constant movement is essential, creating conditions in which vulnerabilities cannot be fully removed but must be continuously managed.
Past incidents, including terrorist attacks and attempted hijackings, were recalled as enduring reference points that continue to influence how security is understood and justified in daily practice. These events were not treated as historical anomalies, but as shared professional experiences that reinforced the need for multiple, overlapping security measures. Background checks, passenger screening systems such as API and PNR, and routine reassessment procedures were described as complementary mechanisms that collectively reduce risk by compensating for one another's limitations.
At the same time, the participant emphasized that effectiveness does not follow automatically from the presence of layered controls. Security measures were described as fragile when applied unevenly or interpreted differently across organizational actors. From this perspective, weaknesses emerged less from the absence of formal procedures than from gaps in coordination, documentation, and shared responsibility. Security effectiveness was therefore understood as dependent on consistent implementation across stakeholders, sustained attention to operational detail, and a collective commitment to maintaining standards over time rather than reliance on any single control or technology.
Vignette 2.Technology as both solution and risk
Participants described technological development in aviation security as a source of both enhanced capability and emerging exposure. Innovations such as biometric identification, facial recognition, artificial intelligence, and unmanned aircraft systems were widely recognized for their contribution to improved detection, faster processing, and expanded monitoring capacity. These tools were associated with greater precision in identifying potential threats and with operational efficiencies that reduce reliance on purely manual controls.
Participants emphasized that technological capability can also introduce new forms of vulnerability when it advances more rapidly than governance structures and professional practice. One account highlighted the role of artificial intelligence in improving screening accuracy and revealing patterns that might otherwise remain unnoticed. This expanded capacity, however, was closely associated with concerns about legal clarity, data protection, and public acceptance, particularly where security technologies extend into areas perceived as intrusive. From this perspective, effectiveness was understood to depend less on technical performance alone than on regulatory alignment and societal trust.
Unmanned aircraft systems were discussed as a further illustration of this tension. Participants described these technologies as expanding the operational environment beyond traditional security perimeters, creating risks that are difficult to manage using existing rules and infrastructure. Where regulatory frameworks lag behind technological diffusion, new opportunities for unlawful interference may emerge.
Across narratives, technology was not framed as a self-contained solution. Its contribution to security was understood as dependent on sustained human oversight, adaptive regulation, and continuous risk assessment. Participants emphasized that technological systems support security objectives only when embedded within clear accountability structures and interpreted by trained professionals capable of responding to unintended consequences as they arise.
Vignette 3.Balancing security, privacy, and human factors
Several participants depicted aviation security as an ongoing effort to reconcile protection requirements with privacy expectations. Cultural diversity, fragmented legal frameworks, and operational constraints across jurisdictions were described as complicating the consistent application of security procedures at airport checkpoints. Within this setting, security measures were experienced not as neutral instruments, but as practices shaped by social norms, legal sensitivities, and public expectations.

Table 4 (continued)

Human factors were described as providing stability within this complex environment. Participants explained that aviation security training operates at two interconnected levels. General security awareness initiatives target all airport personnel, while specialized aviation security training is directed toward those responsible for implementing protective measures. This layered approach was portrayed as central to the development of a shared security culture in which security responsibilities are collectively understood rather than externally imposed. Despite ongoing technological advances, participants consistently emphasized that human judgment remains essential for identifying weak signals, contextual cues, and behavioral irregularities that automated systems may fail to capture.
Vignette 4. Collaboration and the transnational threat landscape
Participants consistently described aviation security as an interdependent system that extends across national borders, institutional boundaries, and regulatory regimes. Security effectiveness was understood as contingent on trust-based cooperation among civil aviation authorities, intelligence agencies, and international organizations. Stable communication channels and timely information exchange were portrayed as essential, particularly in situations where delayed coordination could amplify operational and human consequences.
The contemporary threat environment was characterized as fluid and adaptive rather than static. Insider threats, geopolitical tensions, civil unrest, and challenges related to undocumented passengers were discussed as interconnected risks that evolve across locations and jurisdictions. Participants emphasized that airports and states cannot operate as isolated units, as vulnerabilities in one part of the system can quickly affect others. International frameworks, including ICAO Annex 17, were described as shared reference points that support alignment of national practices and coordinated responses. Insider threats were viewed as especially difficult to detect, arising from gaps in background screening, misuse of access privileges, and internal oversight limitations, thereby requiring sustained vigilance and continuous cooperation rather than episodic intervention.

Acknowledgements All authors have approved the submission of this manuscript.

Author contributions H.C.G. conceived the study, conducted the data collection, and performed the qualitative analysis. E.T. contributed to the theoretical framing and research design. H.K. and A.E.A. provided supervision, contributed to the development of the conceptual framework, and supported the interpretation of the findings. E.E. contributed to the structuring of the manuscript, theoretical integration, and refinement of the discussion and implications. H.C.G. drafted the initial manuscript, and all authors contributed to writing, reviewing, and revising the manuscript. All authors read and approved the final version of the manuscript.

Funding This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability Data supporting the findings of this study are available from the corresponding author (upon reasonable request).

Declarations

Ethical considerations The researchers confirm that all research was conducted in accordance with the relevant guidelines/regulations applicable when human participants are involved. This study was approved by the Ibn Haldun University Scientific Research and Publication Ethics Committee for Social Sciences and Humanities.

Generative AI and AI-assisted technologies in the writing process During the preparation of this work, the authors edited the manuscript using ChatGPT 5 and Grammarly. After using these tools, they reviewed and edited the content as needed and took full responsibility for the content of the published article.

Competing interests The authors declare no competing interests.

References

Abeyratne R (2011) Cyber terrorism and aviation—national and international responses. J Transp Secur 4(4):337–349

Abeyratne R, Abeyratne R (2020) Aviation and cybersecurity in the digital world. In Aviation in the Digital Age: Legal and Regulatory Aspects, 173–211. Springer. https://doi.org/10.1007/978-3-030-48218-3_10

Adey P, Budd L, Hubbard P (2007) Flying lessons: exploring the social and cultural geographies of global air travel. Prog Hum Geogr 31(6):773–791

Agustini E, Kareng Y, Victoria OA (2021) The role of ICAO (International Civil Aviation Organization) in implementing international flight safety standards. KNE Social Sci, 100–114. https://doi.org/10.18502/kss.v5i1.8273

Altheide DL (2007) The mass media and terrorism. Discourse Communication 1(3):287–308

American Educational Research Association (2011) AERA Code of Ethics. Educational Researcher 40(3):145–156. https://doi.org/10.3102/0013189X11410403

Arasly J (2005) Terrorism and civil aviation security: Problems and trends. Connections 4(1):75–90. https://www.jstor.org/stable/26323156

Baker DM (2020) Terrorists' threats to commercial aviation safety and security. In Tourism, Terrorism and Security, 163–181. Emerald Publishing. https://doi.org/10.1108/978-1-83867-905-720201012

Beccaria C (1963) On crimes and punishments (H. Paolucci, Trans. Bobbs-Merrill. (Original work published 1764)

Braun V, Clarke V (2006) Using thematic analysis in psychology. Qualitative Res Psychol 3(2):77–101

British Educational Research Association (2011) Ethical guidelines for educational research. BERA. https://www.bera.ac.uk/publication/ethical-guidelines-for-educational-research

Britannica (2023) Air India Flight 182 disaster. Encyclopaedia Britannica. Retrieved from https://www.britannica.com/event/Air-India-Flight-182-disaster

Bryan E (2018) The culture of surveillance: Watching as a way of life. Social Cult Geogr 19(8):1107–1109. https://doi.org/10.1080/14649365.2018.1525837

Cavoukian A, Jonas J (2012) Privacy by design in the age of big data. https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf

Cleland JA (2017) The qualitative orientation in medical education research. Korean J Med Educ 29:61–71. https://doi.org/10.3946/kjme.2017.53

Cornish DB, Clarke RV (2016) The rational choice perspective. In: Wortley R, Townsley M (eds) Environmental criminology and crime analysis, 2nd edn. Routledge, 29–61

Creswell JW (2009) Research design: Qualitative, quantitative, and mixed methods approaches. Sage

Dawson HG (1987) Civil aviation, hijacking and international terrorism—an historical and legal review. Aeronaut J 91(902):51–63

Denzin NK (2012) Triangulation 2.0. J Mixed Methods Res 6(2):80–88. https://doi.org/10.1177/1558689812437186

Deterding NM, Waters MC (2018) Flexible coding of in-depth interviews. Sociol Methods Res 50(2):708–739. https://doi.org/10.1177/0049124118799377

Duchesneau J, Langlois M (2017) Airport attacks: The critical role airports can play in combatting terrorism. J Airpt Manage 11(4):342–354

Farhaoui Y, Allaoui AE, Amounas F, Mohammed F, Ziani S, Taherdoost H, Bhushan B (2024), November A multi-layered protection system for enhancing data security in cloud computing environments. In The International Conference on Artificial Intelligence and Smart Environment, 559–568. Cham: Springer Nature Switzerland

Fox SJ (2016) Flying challenges for the future: Aviation preparedness–in the face of cyber-terrorism. J Transp Secur 9(3–4):191–218

Fox SJ (2020) The risk of disruptive technology. Technol Soc 62:101304. https://doi.org/10.1016/j.techsoc.2020.101304

Fox SJ (2021) Past attacks, future risks. J Strategic Secur 14(3):112–157

Geertz C (1973) The interpretation of cultures. Basic Books

Gilliam W Jr (2019) Organizational culture in aviation safety. Int J Aviat Aeronaut Aerosp 6(1). https://doi.org/10.15394/ijaaa.2019.1314

Glen A (2014) Aviation terrorism. Secur De?F Q 2(1):59–75

Hadi MA, Closs SJ (2015) Ensuring rigour in qualitative research. Int J Clin Pharm. https://doi.org/10.1007/s11096-015-0237-6
Hall S, McGee JM, Cooper WE (2022) Security and risk assessment. Human Kinetics
Harrison J (2009) International aviation and terrorism: evolving threats, evolving security. Routledge
Hicks N (2016) Project Servator. Ministry of Defence Police
Hodwitz O (2020) Threats to Aviation: Modeling Effectiveness. J Appl Secur Res 15(3):385–407. https://doi.org/10.1080/19361610.2019.1710093
Huang SHS, Hsu WKK, Chen JW (2020) A safety evaluation system based on a revised fuzzy AHP for dangerous goods in airfreights. J Transp Saf Secur 12(5):611–627
Huttunen MT (2021) Bomb threats and civil aviation. J Transp Secur 14(3–4):291–306. https://doi.org/10.1007/s12198-021-00235-5
Hyvärinen M (2008) Analyzing narratives and story-telling. Sage Handb social Res methods 1:447–460
International Civil Aviation Organization (2017) Annex 17: Security. ICAO
Jackson BA, Chalk P, Cragin K, Newsome B, Parachini JV, Rosenau W, Simpson EM, Sisson MW, Temple D (2007) Breaching the fortress wall. RAND Corporation
Jackson BA, Chan EW, LaTourrette T (2012) Trusted traveler programs. J Transp Secur 5:1–34
Jager A (2018) The shoe bomber Richard Reid. International Institute for Counterterrorism
Jenkins BM (2017) The challenge of protecting transit. Mineta Transportation Institute
Juvan J, Prezelj I, Kopač E (2021) Public dilemmas about aviation security. Secur J 34:410–428. https://doi.org/10.1057/s41284-020-00240-8
Karatsareas P (2022) Semi-structured interviews. Cambridge University Press. https://doi.org/10.1017/9781108867788.010
Kaunert C, Callander B, Léonard S (2022) The collective securitization of aviation in the European Union through association with terrorism. Collective Securitization and Crisification of EU Policy Change. Routledge, 61–78
Kiger ME, Varpio L (2020) Thematic analysis. Med Teach 42(8):846–854. https://doi.org/10.1080/0142159X.2020.1755030
Kirschenbaum AA, Mariani M, Van Gulijk C, Lubasz S, Rapaport C, Andriessen H (2012) Airport security: An ethnographic study. J Air Transp Manage 18(1):68–73. https://doi.org/10.1016/j.jairtraman.2011.10.002
Klenka M (2019) Major incidents shaping aviation security. J Transp Secur 12(1–2):39–56. https://doi.org/10.1007/s12198-019-00201-2
Klenka M (2021) Aviation cyber security: legal aspects of cyber threats. J Transp Secur 14(3–4):177–195
Komasová S (2020) Airport security and visibility: security as visualization and its in-place performance. J Appl Secur Res 15(3):332–354. https://doi.org/10.1080/19361610.2020.1738315
Krull KE (2016) The threat among us: Insiders intensify aviation terrorism. PNNL
Lacey D (2010) Understanding and transforming organizational security culture. Inform Manage Comput Secur 18(1):4–13
Lincoln YS, Guba EG (1985) Naturalistic inquiry. Sage Publications
Loffi JM, Wallace RJ (2014) The unmitigated insider threat to aviation (Part 1): A qualitative analysis of risks. J Transp Secur 7(4):289–305
Low JM, Yang KK (2019) An exploratory study on the effects of human, technical and operating factors on aviation safety. J Transp Saf Secur 11(6):595–628
Maitlis S, Lawrence TB (2007) Triggers and enablers of sensegiving in organizations. Acad Manag J 50(1):57–84
Merhi MI, Ahluwalia P (2019) Deterrence factors and IS security. Comput Hum Behav 92:37–46. https://doi.org/10.1016/j.chb.2018.10.031
Miles MB, Huberman AM, Saldaña J (2014) Qualitative data analysis: A methods sourcebook, 3rd edn. Sage Publications
Morral AR, Jackson BA (2014) Understanding the role of deterrence in counterterrorism security. Rand Corporation. http://www.rand.org/pubs/monographs/MG481/
Nagin DS (2013) Deterrence: A review of the evidence. Annual Rev Econ 5(1):83–105
National Research Council (US) Transportation Research Board. Committee for a Study of Public-Sector Requirements for a Small Aircraft Transportation System. (2002). Future flight: a review of the small aircraft transportation system concept

Nikolaev AG, Lee A, Jacobson S (2012) Optimal aviation security screening strategies with dynamic passenger risk updates. IEEE Trans Intell Transp Syst 13(1):203–212
Nugraha RA, Choi J (2016) Body scanners: Security or privacy issue? Aviat Space J 15(3)
Osborne N, Grant-Smith D (2021) In-depth interviewing. Springer. https://doi.org/10.1007/978-981-16-1677-8_7
Oster CV Jr, Strong JS, Zorn CK (2013) Analyzing aviation safety: problems, challenges, opportunities. Res Transp Econ 43(1):148–164
Pettersen KA, Bjørnskau T (2015) Organizational contradictions between safety and security–Perceived challenges and ways of integrating critical infrastructure protection in civil aviation. Saf Sci 71:167–177. https://doi.org/10.1016/j.ssci.2014.04.018
Pilarska J (2021) Constructivist paradigm. Multilingual Matters
Pita J et al (2009) Deployed security games. AAAI
Price J, Forrest J (2016) Practical aviation security. Butterworth-Heinemann
Price J, Forrest J (2024) Practical aviation security: predicting and preventing future threats. Elsevier
Roach K (2011) The Air India report and the regulation of charities and terrorism financing. Univ Tor Law J 61(1):45–57
Robinson OC (2013) Sampling in interview-based research. Qualitative Res Psychol 11(1):25–41
Roulston K (2017) Qualitative interviewing. Qualitative Res 18(3):322–341
Sakano R, Obeng K (2016) Airport screening satisfaction. J Air Transp Manage 55:129–138
Salter MB (2008) Politics at the airport. University of Minnesota Press
Schóber T, Koblen I, Szabo S (2012) Present and potential security threats posed to civil aviation. Incas Bull 4(2):169–175. https://doi.org/10.13111/2066-8201.2012.4.2.17
Sinai J (2012) New trends in airport and aviation security. J Counterterrorism Homel Secur Int 18(3):30–37
Singh S, Singh M (2003) Explosives detection systems (EDS) for aviation security. Sig Process 83(1):31–55
Stewart MG, Mueller J (2011) Cost–benefit analysis of body scanners. J Homel Secur Emerg Manage 8(1):30
Stewart, M. G., & Mueller, J. (2008). Assessing the risks, costs and benefits of United States aviation security measures.
The Canadian Encyclopedia (2023) Air India Flight 182 Bombing. Retrieved from https://www.thecanadianencyclopedia.ca/en/article/air-india-flight-182-bombing
Tomlinson KD (2016) An examination of deterrence theory: Where do we stand. Fed Probat 80(3):33–38
Tuman JS (2009) Communicating terror: The rhetorical dimensions of terrorism. Sage Publications
Uzulmez M, Ates SS (2017) Terrorist attacks in aviation: An analysis of Ataturk Airport attack on 28th of June 2016. PressAcademia Procedia 3(1):1012–1018. https://doi.org/10.17261/Pressacademia.2018.773
van Hulst M, Tsoukas H (2023) Understanding extended narrative sensemaking: how police officers accomplish story work. Organization 30(4):730–753
Willison R, Lowry PB, Paternoster R (2018) A tale of two deterrents: considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research. J Assoc Inf Syst 19(12):1187–1216. https://doi.org/10.17705/1jais.00524
Wilson A (2015) A guide to phenomenological research. Nurs Standard (2014+) 29(34):38
Wong S, Brooks N (2015) Evolving risk-based security: A review of current issues and emerging trends impacting security screening in the aviation industry. J Air Transp Manage 48:60–64
Yao W, Chu CH, Li Z (2012) The adoption and implementation of RFID technologies in healthcare: A literature review. J Med Syst 36:3507–3525
Zilincik S, Sweijs T (2023) Beyond deterrence. Contemp Secur Policy 44(2):248–275. https://doi.org/10.1080/13523260.2023.2185970

Authors and Affiliations

Hanan China Gahwita[1] · Ekrem Tatoglu[2,3] · Halit Keskin[4] · Ali E. Akgün[4] · Emel Esen[4]

✉ Emel Esen
emeloz@yildiz.edu.tr

Hanan China Gahwita
hanan.gahwita@stu.ihu.edu.tr

Ekrem Tatoglu
tatoglu.e@gust.edu.kw; ekrem.tatoglu@ihu.edu.tr

Halit Keskin
hkeskin@yildiz.edu.tr

Ali E. Akgün
aakgun@yildiz.edu.tr

1 School of Graduate Studies, Ibn Haldun University, Basaksehir, Istanbul 34480, Turkey

2 College of Business Administration, GUST Center for Sustainable Development (CSD), Gulf University for Science & Technology, West Mishref, 32093 Kuwait City, Kuwait

3 Department of Management, School of Business, Ibn Haldun University, Basaksehir, Istanbul 34480, Turkey

4 Department of Management, Faculty of Economics and Administrative Sciences, Yildiz Technical University, Istanbul 34220, Turkey