Revista Perspectivas en Inteligencia
(Scientific Journal of Social Sciences and Interdisciplinary Studies)
Volume 18, Number 27, January - June 2026
ISSN: 2145-194X (printed), 2745-1690 (online)
Website: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem

Authors:

Oscar Alberto Rojas-Martínez
https://orcid.org/0000-0002-3826-2706
✉ nacho_rojas07@hotmail.com
Escuela de Aviación del Ejército, Colombia

Heivar Yesid Rodríguez-Pinzón
https://orcid.org/0000-0002-9553-0455
✉ rodriguezphy@javeriana.edu.co
Pontificia Universidad Javeriana, Colombia

APA Citation: Rojas-Martínez, O. A. & Rodríguez-Pinzón, H. Y. (2026). Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem. *Perspectivas en Inteligencia, 18*(27), 75-97. http://doi.org/10.47961/2145194X.860

Published online: 2026

To submit an article:
https://revistaseditorialejc.org/index.php/pei/about/submissions

This page is intentionally left blank

PERSPECTIVAS EN INTELIGENCIA 2026

Revista Científica en Ciencias Sociales e Interdisciplinaria
Volume 18, Number 27, January - June 2026, pp. 75-97
ISSN 2145-194X (printed), 2745-1690 (online)
Bogotá, D. C., Colombia
http://doi.org/10.47961/2145194X.860

Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem

Sistemas Antidrones para la seguridad aérea en el ecosistema de la aviación civil colombiana

Oscar Alberto Rojas-Martínez[1] & Heivar Yesid Rodríguez-Pinzón[2]*

(1) Escuela de Aviación del Ejército, Bogotá, D. C., Colombia,
✉ nacho_rojas07@hotmail.com

(2) Pontificia Universidad Javeriana, Bogotá, D. C., Colombia,
✉ rodriguezphy@javeriana.edu.co

* Author to whom the correspondence is addressed

Abstract

In the era of the Fourth Industrial Revolution, the widespread adoption of emerging technologies across industries and society has fostered innovation in multiple processes. However, the misuse of certain technologies, particularly unmanned aerial vehicles (UAVs), has generated new risks and threats for different sectors due to limited governmental oversight and operational control. These risks may negatively affect society, industries, civil aviation, institutional stability, and ultimately the State itself. Within the Colombian aviation ecosystem, this study analyzes the impact of drones on comprehensive airport security, focusing on potential scenarios that threaten physical security and operational safety through the malicious use of advanced technologies, in some cases supported by artificial intelligence (AI). Using a preliminary interpretive approach, the research aims to examine the relevance of anti-drone technologies in Colombia from both aviation safety and security perspectives, contributing to the strengthening of these essential pillars for global air transport operations. Finally, by contextualizing the problem, this study contributes to the body of knowledge on anti-drone systems, their necessity, applications, and regulatory frameworks, drawing on national and international research experiences to assess operational contexts, determine their strategic importance, and highlight some of their advantages.

Classification JEL: H56, L93, O33.

Keywords: aviation safety; aviation security; surveillance systems; civil aviation; airport security; technological change.

Date received: 09/05/2026 | Date Accepted: 02/08/2026

Resumen

En la era de la cuarta revolución industrial, la adopción generalizada de tecnologías emergentes en las industrias y la sociedad ha impulsado la innovación en múltiples procesos. Sin embargo, el uso indebido de ciertas tecnologías, particularmente los vehículos aéreos no tripulados (UAV), ha generado nuevos riesgos y amenazas para diferentes sectores debido a la limitada supervisión gubernamental y al control operacional insuficiente. Estos riesgos pueden afectar negativamente a la sociedad, las industrias, la aviación civil, la estabilidad institucional y, en última instancia, al propio Estado. Dentro del ecosistema de la aviación colombiana, este estudio analiza el impacto de los drones en la seguridad aeroportuaria integral, enfocándose en escenarios potenciales que amenazan la seguridad física y la seguridad operacional mediante el uso malicioso de tecnologías avanzadas, en algunos casos apoyadas en inteligencia artificial (IA). Mediante un enfoque interpretativo preliminar, la investigación busca examinar la relevancia de las tecnologías antidrones en Colombia desde las perspectivas de seguridad operacional y seguridad física de la aviación, contribuyendo al fortalecimiento de estos pilares esenciales para las operaciones globales de transporte aéreo. Finalmente, al contextualizar el problema, este estudio contribuye al cuerpo de conocimiento sobre los sistemas antidrones, su necesidad, aplicaciones y marcos regulatorios, apoyándose en experiencias de investigación nacionales e internacionales para evaluar contextos operacionales, determinar su importancia estratégica y resaltar algunas de sus ventajas.

Palabras clave: seguridad operacional de la aviación; seguridad de la aviación; sistemas de vigilancia; aviación civil; seguridad aeroportuaria; cambio tecnológico.

Introduction

This article examines the need to implement anti-drone systems in Colombian civil and commercial aviation, with particular emphasis on the safe operation of airports in response to the increasing use of unmanned aerial vehicles (UAVs) that are not fully regulated by the national aviation authority. The implementation of such systems has become imperative to address an emerging and evolving threat, as well as to ensure the safety and continuity of civil air operations in Colombia. In this context, technological solutions capable of mitigating the risks associated with the misuse of drones in restricted and sensitive areas are analyzed.

Accordingly, it is essential to explore how anti-drone technologies can be effectively integrated into existing aviation security protocols in order to protect the civil aviation ecosystem and ensure comprehensive airport management across the country. In recent years, the rapid expansion of the unmanned aircraft market has been accompanied by the advancement of Artificial Intelligence (AI), which has enhanced the capabilities, autonomy, and range of applications of these aerial platforms. This convergence has generated new operational possibilities, while simultaneously introducing complex challenges for aviation safety and security.

Within this scenario, aviation authorities play a central role as the primary regulatory and supervisory bodies responsible for the use and integration of UAVs into national

airspace. As defined by Choi (2022), unmanned aircraft can be understood as "independent bodies" that represent a paradigm shift, exceeding traditional industry standards and evolving as a core technology interconnected with other emerging technologies (p. 1).

The growing use of drones has consequently posed significant challenges to aviation ecosystems. Although initially designed for recreational and commercial purposes, UAVs and their associated systems have increasingly been employed for malicious activities, posing potential threats to civil aviation operations. The uncontrolled commercial growth of drone sales may result in airspace interference, mid-air collisions, violations of privacy, and risks to critical infrastructure, among other safety and security concerns.

In this regard, it is necessary to examine whether the implementation of anti-drone systems in Colombian civil aviation can effectively mitigate risks and reduce threats associated with the misuse of UAVs, without adversely affecting aviation operations or technical systems (Jačionis, 2020). This research is therefore both relevant and necessary, as it responds to current protection demands in Colombian airports and seeks to contribute to the development of a safer operational environment. Furthermore, the deployment of such systems may strengthen the overall resilience of the aviation ecosystem against emerging security challenges.

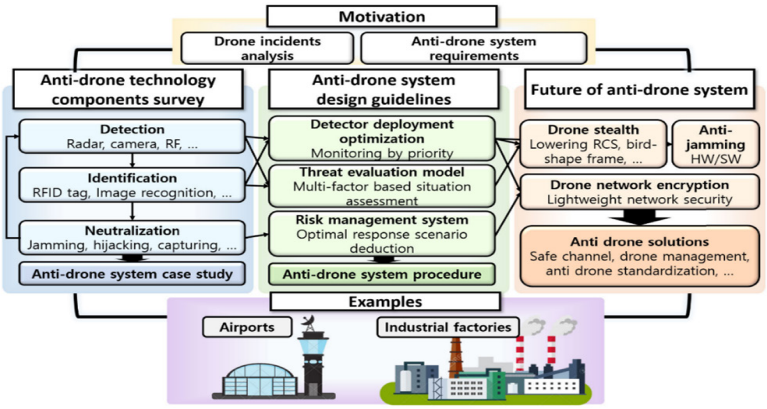
Based on a qualitative literature review on anti-drone systems and aviation security, this study aims to contribute to a deeper understanding of the current state and relevance of drones as a research phenomenon within civil aviation. Data collection and analysis are conducted within an interpretative paradigm, allowing for the assessment of the impact of unmanned aircraft on air security and the evaluation of potential countermeasures for their unregulated operation. This methodological approach supports the organization of the study into epistemological, theoretical, methodological, and results-oriented components.

Finally, the review of existing academic literature highlights the contribution of the Colombian National Army Aviation School (ESAVE), as a higher education institution within the aviation sector, through its presentation entitled Anti-Drone Systems: A Necessity for the Comprehensive Security of the Colombian Civil Aviation Ecosystem. This contribution provides a broad perspective on the phenomenon affecting air security and serves as a key motivation for the present manuscript, recognizing anti-drone systems as a pertinent, timely, and highly relevant topic currently demanded by the aviation industry.

Background and security context of unmanned aircraft systems

The increasing security challenges affecting aeronautical, industrial, and social ecosystems as a result of the rapid expansion of unmanned aircraft have led to the identification of a structured roadmap, as illustrated in Figure 1.

Figure 1. Roadmap for anti-drone system design and development



Source: Park et al. (2021)

This roadmap, developed across three main domains, reflects the general spectrum proposed by Park et al. (2021) and facilitates an understanding of the comprehensive landscape surrounding the relevance of anti-drone systems. It ranges from the motivations behind contemporary drone attacks to the prospective evolution of these aircraft and their implications for security and protection, highlighting the growing need for technological solutions capable of countering malicious drone activities (Chávez & Swed, 2021).

As shown in Figure 1, the use of unmanned aircraft influences a wide range of industries, particularly within non-military contexts where technological development is often more dynamic. From a civil aviation perspective, this evolving ecosystem presents complex operational and security challenges that must be addressed to ensure the protection of air transport systems.

Drones, also referred to as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UAS), are robotic platforms capable of operating autonomously or through various control mechanisms, including remote controllers, mobile devices, and advanced human–machine interfaces. Until the early 2000s, these systems were predominantly military assets and largely inaccessible to civilians. However, advances in hardware and software technologies have enabled the development of smaller, more affordable, and easier-to-operate platforms (Tezza & Andujar, 2019), leading to their widespread civilian adoption.

From a security perspective, the rapid proliferation of drones has introduced significant concerns. As noted by Balladares et al. (2024) and Kang et al. (2021), the increasing presence of drones requires a deeper understanding of their operational implications, as technological progress is now primarily constrained by human creativity and ethical considerations rather than technical limitations. Consequently, drones have become ubiquitous elements within modern societies.

Within the context of the Fourth Industrial Revolution, drones may generate adverse

effects on public safety. Hwang & Kim (2020) describe them as "an attractive tool for criminal and terrorist groups because they can be equipped with weapons at low cost, conceal their operators, and evade surveillance equipment" (p. 248). Table 1 summarizes several documented incidents involving the malicious use of drones across different industries and critical infrastructure sectors, underscoring the seriousness of this emerging threat.

Table 1 provides a brief compilation of selected global cases of drone misuse. In the aviation sector, such threats are associated with airspace interference, near-miss events, and collision risks, many of which remain underreported due to regulatory gaps, limited data availability, and the relatively recent integration of drones into civil airspace. As Shin et al. (2021) emphasize, the growth in unauthorized drone operations increases the likelihood of accidents, property damage, and intentional harm. Consequently, when illegal drone activity is detected in the vicinity of airports, immediate action is required to ensure aviation safety (Hwang & Kim, 2020).

Table 1. Selected global cases of drone-related incidents affecting critical infrastructure and aviation

Date	Country	Event Details
January, 2015	USA	In Washington D.C., a civilian UAV flew over the White House fence and crash-landed on the lawn.
April, 2015	JAPAN	Phantom 2 drone carrying traces of radiation was found on the roof of the Japanese Prime Minister's Official Residence.
October, 2016	Iraq	ISIS may have used a commercial drone rigged with explosives to kill two Kurdish Peshmerga soldiers and wound two French soldiers in Iraq.
August, 2016	South Africa	A small UAV crashed into a nuclear powerplant in Koeberg.
August, 2018	Venezuela	Two drone bombs used in an attempt to assassinate President Nicolas Maduro.
December, 2018	United Kingdom	Two drones found at Gatwick airport. The airport's closure led to more than 100,000 people being stranded or delayed.
September, 2019	Saudi Arabia	Two major Saudi oil installations hit by drone strike. Production of 5.7 million barrels a day was suspended.

Source: Reproduced from Hwang & Kim (2020)

In light of this context, the implementation of anti-drone systems has become a critical requirement for the Colombian civil aviation ecosystem. Such systems must be integrated into existing operational and industrial frameworks in a manner that safeguards both aviation safety and civil aviation security, while accommodating the continuous technological evolution of unmanned aircraft.

Airports and Drones

Within the context of Industry 4.0, technological advancements have significantly lowered the barriers to accessing and operating unmanned aerial vehicles (UAVs), enabling individuals and organizations to acquire drone-related skills for recreational, commercial, and mission-specific purposes. This accessibility has transformed the long-standing human aspiration of flight into a widely attainable capability through unmanned aviation. While these developments have fostered innovation across multiple scientific and industrial fields, they have also introduced new operational and security challenges, particularly within airport environments (Sichko, 2019).

The current era has been described as the "Drone Age", a concept articulated by Boyle (2020) to capture the rapid evolution and widespread availability of drone technologies for both state and non-state actors. Drones have progressed from simple reconnaissance platforms to highly capable systems able to conduct complex missions with minimal human intervention. This evolution raises ethical, legal, and regulatory concerns related to accountability, privacy, and oversight, as the diversity of drone applications increasingly intersects with fundamental human and societal values (Završnik, 2016).

From an aviation security perspective, the proliferation of UAVs has exposed airports to a range of emerging vulnerabilities, including cyber-related threats and operational disruptions. As highlighted by Costin et al. (2023) and Hurtado-Cubillos (2022), the growing dependence on unmanned systems across multiple sectors expands the attack surface of critical infrastructure, necessitating more robust and integrated security management approaches. Despite this reality, academic research has historically focused more on the technical development and operational capabilities of drones than on the identification of effective countermeasures or airport-specific mitigation strategies.

Only in the second decade of the 21st century has scholarly attention increasingly shifted toward regulatory and operational challenges associated with unmanned aviation. As noted by Merkert & Bushell (2020), contemporary aviation issues have expanded beyond traditional regulatory concerns to encompass novel risks that had not previously been encountered. In airport contexts, the misuse of drones represents a particularly disruptive threat, facilitated by their remote operation, low cost, and ease of access. Consequently, proactive airport security management requires systematic threat identification and scenario-based risk assessment, as emphasized by Cole (2014).

Airports operate under the assumption of persistent exposure to evolving threats, requiring continuous adaptation of mitigation strategies and security systems. While past approaches often focused on the detection of prohibited objects, there has been a gradual shift toward identifying malicious actors and intent. This transition reflects a broader movement toward intelligence-led and risk-based security management models that enhance decision-making and operational resilience.

The integration of drones into airport operations has further complicated this landscape. In recent years, controlled drone operations within airport environments have been introduced under strict regulatory conditions, including predefined corridors and restricted

zones to enable coexistence with commercial aviation (Shvetsova & Shvetsov, 2021). Nevertheless, collision risks remain, particularly during critical flight phases such as takeoff, approach, and taxiing, where manned aircraft operate at low altitudes. As La Cour-Harbo & Schiøler (2019) note, even when drones operate below 500 feet, residual risks persist within controlled aerodromes.

In Colombia, civil aviation oversight is exercised by the Special Administrative Unit of Civil Aeronautics, which is responsible for developing, interpreting, and enforcing civil aviation regulations. As a contracting State of the Convention on International Civil Aviation (Chicago Convention, December 7, 1944.), Colombia is a member of the International Civil Aviation Organization and is committed to implementing its standards and recommended practices, including those related to pilotless aircraft as addressed in Article 8 of the Convention (Law No. 12 of 1947).

In response to the growing relevance of unmanned aviation, Colombia has advanced strategic initiatives through its aviation authority, including the Action plan of the Unmanned Aviation Strategic Plan 2023-2026. This framework aims to support the safe and orderly integration of unmanned aircraft into national airspace, as illustrated in Figure 2, which outlines the corresponding action plan.

Figure 2 . Action plan of the Unmanned Aviation Strategic Plan 2023-2026

Source: (Unidad Administrativa Especial de Aeronáutica Civil de Colombia, 2023)

These measures are complemented by national regulations, such as RAC 100, which governs the operation of unmanned aircraft systems (UAS) within the Colombian aviation system.

Despite these efforts, regulatory and institutional frameworks alone are insufficient to fully address the risks associated with malicious drone activities. As emphasized by Hwang & Kim (2020), while legal mechanisms are necessary to enable legitimate drone operations, it is equally critical to protect national critical infrastructure from hostile or unlawful uses. The continuous evolution of drone technologies requires that regulatory systems remain dynamic and adaptive, supported by the development and implementation of anti-drone systems capable of detecting and neutralizing unauthorized UAVs across diverse operational scenarios.

Integrated Aviation Safety and Security

The integration of aviation safety and security presents a persistent challenge for airport management, particularly in the context of rapid technological evolution and increasing system complexity. The interaction between theory and practice requires adaptive strategies capable of addressing both accidental hazards and intentional threats within the aviation ecosystem. Although safety and security share common objectives, they differ in their technical focus, methodological approaches, and operational implications, as highlighted by Pettersen-Gould & Bieder (2020). As these authors argue, maintaining the effectiveness of safety-related defenses is essential for protecting hazardous technologies, given their reliance on past incidents and the dynamic, yet fragile, organizational structures that support them.

From a security perspective, the primary challenge lies in identifying and managing risks associated with hostile intent, manifested through internal or external acts of sabotage. As noted by Schulman (2020), a fundamental distinction between safety and security management lies in the primacy of malicious intent in security-related threats. This distinction is increasingly relevant in aviation, where societal trends and technological adoption often outpace regulatory and organizational responses, creating vulnerabilities within critical infrastructure such as airports.

These vulnerabilities are further exacerbated by the growing exposure of aviation systems to cyber threats. Cyberattacks targeting data integrity, communication networks, and operational platforms represent a significant concern for both safety and security management. As Schulman (2020) observes, the progressive incorporation of digital components into complex systems introduces additional layers of vulnerability, complicating the processes of risk forecasting and system comprehension. In aviation, where connectivity across multiple dimensions is essential, this cyber–physical interdependence amplifies the potential impact of malicious actions.

Within airport environments, the management of unmanned aircraft systems illustrates the limitations of traditional approaches to safety and security. As noted by Merkert & Bushell (2020), some airports have implemented measures to manage drone activity within their airspace; however, many of these approaches remain reactive or defensive in nature. Literature increasingly emphasizes the need for proactive and preventive management stra-

tegies that integrate safety and security considerations into a unified operational framework.

Academic definitions of safety and security commonly distinguish between the two based on intentionality and systemic orientation. Safety primarily addresses unintentional hazards and accidental risks, focusing on the system's capacity to avoid causing harm to its environment. In contrast, security is concerned with intentional threats and malicious actions, emphasizing the system's ability to withstand harm originating from its environment (Pettersen-Gould & Bieder, 2020). These distinctions underscore the necessity of coordinated management approaches capable of addressing both dimensions simultaneously.

From the perspective of airport user protection and operational resilience, Bongiovanni (2020) synthesizes these approaches by highlighting the legal and managerial dimensions of risk management through both differential and collaborative models. This synthesis, presented in Table 2, illustrates how safety and security measures can be aligned within airport management systems to enhance decision-making and organizational coordination.

Table 2. Approaches to safety and security in airports: a synthesis

Airport safety and security	Legal approach	Managerial approach	Design approach
Focus	Law	Resources/goals	Users
Mission	Zero unintentional accidents (safety); zero intentional incidents (security)	Efficiently mitigate risks	Delight users
Driver for innovation	Changes in societal practices cause regulations to change	Changes in regulations, business goals, and budget cause managerial practices to change	Changes in users' needs and jobs to be done change experience design
Lead-innovator	Legislator	Enlightened manager	User experience designer
Innovation source	Top-down	Top-down/bottom-up	Bottom-up
Should safety and security be separated or combined?	Separation: two different regimes	Separation/combination: depending on resources and goals	Combination: both are components of users' experience
Overarching question	"We need to meet specific standards in terms of safety and security events happening in the airport"	"We need to be compliant to regulations together with employing the most efficient mix of resources and achieving our business goals"	"We need to make safety and security a memorable experience for our users"

Source: Reproduced from (Bongiovanni, 2020, p. 60)

Despite the development of robust safety cultures, security risks often remain beyond the full control of organizations. External threats, such as terrorism or coordinated cyber-physical attacks, may materialize regardless of internal preparedness and are not necessarily linked to economic performance or production systems (Jore, 2020). Consequently, even well-managed organizations may experience severe disruptions resulting from security breaches.

Finally, the protection of critical air transport infrastructure against combined physical and cyber threats requires integrated management cycles that bridge safety and security functions. As emphasized by Mantzana et al. (2020), enhancing interoperability among existing systems and aligning physical and digital protection mechanisms are essential steps toward developing more resilient and adaptive aviation security solutions.

Methodology

Building on the research question, "How can anti-drone technologies be effectively integrated into existing security protocols to protect the civil aviation ecosystem and ensure comprehensive management in Colombian airports?", this study adopts a qualitative research approach based on systematic observation and documentary analysis. The research design is descriptive in nature and focuses on the identification, classification, and interpretation of academic and technical sources related to unmanned aircraft systems, aviation security, and counter-drone technologies.

The documentary analysis was conducted using specialized academic databases, including Scopus, EBSCOhost, and Google Scholar. The primary selection criteria prioritized peer-reviewed publications released between 2019 and the first semester of 2024, with limited exceptions made for earlier works considered highly relevant to the analytical framework. The reviewed literature is largely drawn from indexed journals specializing in aviation, aerospace systems, and security studies, as reflected in the reference list.

The methodological process followed three structured phases planning, execution, and completion adapted from the framework proposed by Niño-Rojas (2011). During the planning phase, the phenomenon under study was defined and the literature was systematically organized into three analytical categories: Airports and Drones, Integrated Aviation Security (safety–security), and Anti-Drone Systems as a Management Tool for Aeronautical Security.

The execution phase involved data processing, qualitative analysis, and interpretative synthesis of the selected sources, allowing for the identification of patterns, challenges, and emerging trends in the integration of counter-drone systems within airport security environments. Finally, the completion phase consisted of consolidating the analytical findings into a structured academic manuscript.

This methodological approach is grounded in an interpretive paradigm, drawing upon the researcher's empirical, academic, and ethical expertise. The interpretive perspective is considered appropriate for analyzing the evolving technological and regulatory lands-

cape of unmanned aircraft systems and anti-drone solutions, recognizing the dynamic and still-developing nature of knowledge in this domain.

Anti-drone systems for aviation safety management

Current drone detection systems used in aviation environments present operational limitations, making it necessary to assess the probability of threat detection under varying operational and environmental conditions. As noted by Łukasiewicz & Kobaszyńska-Twardowska (2022), these systems, "composed of devices operating on diverse principles, should be constructed based on the probability of detecting a drone under established conditions" (p. 96). Consequently, both the operational characteristics of unmanned aircraft and the contextual conditions of their deployment directly influence the effectiveness of preventive and neutralization measures.

From an operational perspective, it is essential to consider systems capable of identifying risks posed by both individual drones and coordinated drone swarms. This requires an analytical approach supported by probabilistic and experimental models that address the increasing autonomy and adaptability of unmanned aircraft. As highlighted by Öz & Sert (2019), emerging generations of drones pose significant challenges, particularly in relation to "complete situational awareness of airspace and the automatic execution of all types of missions" (p. 706). In this context, organizations face the fundamental question of how to protect critical aviation infrastructure against such agile and heterogeneous threats.

Importantly, the risks associated with malicious drone operations are not limited to physical intrusion. Cyber-related threats, including electronic interference and signal manipulation, have emerged as critical vulnerabilities affecting airports and other elements of national critical infrastructure. In response, the formal management of aviation security has become a standard requirement within international civil aviation. The implementation of Security Management Systems (SeMS), supported by Safety Management Systems (SMS), is currently regarded as best practice for addressing both physical and cyber-related threats, as emphasized by Stastny & Stoica (2022). In this context, Table 3 presents proposed measures aimed at enhancing the effectiveness of ATM-related SMS in the management of cybersecurity risks.

Table 3. Proposed measures to enhance ATM Safety Management System (SMS) effectiveness in addressing cybersecurity threats

SMS Elements	*Potential Organisational Vulnerability/Need*	Proposed Counter-Measures for SMS Enhancement
Safety Policy	Organisation insufficiently aware of need for defence against cybersecurity threats.	Incorporate the need to reinforce the SMS and support the SeMS within the organisation's safety policy.
Organisational Safety Responsibilities	Key personnel are unaware of their roles and responsibilities in respect of cybersecurity threats.	Define roles and responsibilities for key safety personnel in respect of cybersecurity threats, and the need to liaise with and support organisational security management personnel.

SMS Elements	Potential Organisational Vulnerability/Need	Proposed Counter-Measures for SMS Enhancement
Coordination of Emergency Response Plan (ERP)	Emergency Response Plan unprepared to cope with cyber-attacks.	Include cyber-attacks as a source of actual or potential disruption to be managed within the scope of the ERP.
Risk Management Process	Need to consider cybersecurity threats to safety alongside all other risks.	Include cybersecurity threats within the safety risk assessment and mitigation process, including a means of risk categorisation. Co-assurance methodologies (ref. para 6 above) may be used if consistent with the means of documenting safety arguments (e.g. use of safety cases).
Safety Interfaces	Need to ensure that SMS actions taken in respect of countering cybersecurity effects on safety are fully coordinated within the organisation.	Implement procedures to ensure full coordination between SMS responses to cybersecurity threats and wider organisational functions, including security management.
Safety Performance Monitoring	All threats to ATM safety need to be monitored to establish the scale and nature of the threats, as well as longer term trends.	Update performance monitoring procedures to include the effects of cybersecurity threats on ATM safety performance.
Continual SMS Improvement	SMS must be kept current in terms of known or anticipated threats to safety.	Updated assessments of cybersecurity threats to be taken into account as part of regular SMS effectiveness reviews.
Safety Reporting	Need to achieve full visibility of cybersecurity occurrences and their effect on safety performance.	Introduce further categorisation within the safety reporting system to take account of cybersecurity events, including a means of severity classification (in terms of safety impact).
SMS Audits	To ensure that cybersecurity counter-measures are in place and functioning effectively.	To include SMS measures to counter cybersecurity threats in regular SMS audits.
Safety Communication	Cybersecurity issues and events need to form part of normal organisational communications (internal and external) on safety matters.	To improve organisational awareness by including cybersecurity information within normal communications methods on safety matters.
Training and Education	A key need is awareness of cybersecurity threats and defences at all levels of the organisation.	To formalise awareness of cybersecurity matters through their inclusion in organisational training programmes.

Source: Reproduced from (Stastny & Stoica, 2022, p. 8)

With regard to technological solutions, currently available anti-drone systems despite their limitations commonly rely on radar-based detection, acoustic interception, infrared sensors, and electro-optical devices (Popescu, 2021; Semenyuk et al., 2025). Detection remains the primary enabling function, as it supports subsequent processes of recognition, identification, and localization, forming the foundational architecture of any counter-drone system. Within airport environments, the effective management of these technologies requires an integrated assessment of the electromagnetic spectrum, the physical layout of operational and administrative facilities, and the characteristics of controlled airspace, as noted by Mackie & Lawrence (2019) and Pérez-Herrera (2013). This holistic approach is essential not only for system implementation, but also for fostering an organizational security culture oriented toward the integrity and resilience of aviation protection systems.

Findings

The analysis indicates that the rapid expansion of unmanned aerial vehicles (UAVs) in the 21st century has significantly outpaced the capacity of the aviation sector to anticipate and regulate their operational implications. The widespread commercial availability and diversification of drone applications have accelerated their integration into air operations, while simultaneously increasing regulatory complexity and enforcement challenges.

A key finding of this study is that anti-drone systems are increasingly understood not merely as technological countermeasures, but as integral components of aviation safety and security management systems. The reviewed literature highlights that the effectiveness of such systems depends on their integration within structured management frameworks rather than on standalone technological solutions.

The findings also reveal that risks associated with drone operations extend beyond physical intrusion, encompassing cyber-related threats, privacy violations, and disruptions to airport operations. These risks are amplified in operational environments where detection, identification, and response capabilities are limited or insufficiently coordinated.

Furthermore, the analysis shows that regulatory instruments and technical standards alone are insufficient to ensure comprehensive protection against malicious or unregulated drone activities, particularly in complex airport environments. Instead, effective mitigation requires coordinated detection and response mechanisms adapted to the operational characteristics of each airport.

In the specific context of Colombian airports, the findings indicate that no single anti-drone technology is capable of effectively mitigating all potential threats. Rather, the integration of multiple complementary systems aligned with local technological infrastructure, airspace characteristics, personnel capabilities, and organizational context emerges as a necessary condition for managing drone-related risks and safeguarding the civil aviation ecosystem.

Discussion

The integration of unmanned aircraft into the aviation ecosystem has fundamentally reshaped not only operational practices, but also regulatory and security paradigms. The findings of this study highlight the growing gap between rapid technological innovation and the capacity of regulatory and management frameworks to respond effectively to emerging risks. In this context, anti-drone systems emerge not solely as technological solutions, but as critical enablers of aviation safety and security governance.

The discussion reveals that the accelerated adoption of drone technologies has challenged traditional regulatory approaches, which have struggled to adapt at the same pace as technological development. This imbalance has contributed to regulatory fragmentation and uneven enforcement, particularly in complex environments such as airports. From this perspective, the application of analytical frameworks such as game theory helps to illustrate the strategic interaction between drone operators, regulatory authorities, and security stakeholders, underscoring the adaptive and dynamic nature of contemporary airspace threats.

These findings suggest that regulatory agencies must move beyond reactive rulemaking toward anticipatory and adaptive regulatory models. Proactive frameworks that account for future technological developments would facilitate the safe integration of drones into controlled airspace while reducing vulnerabilities associated with malicious or unauthorized operations. Within this regulatory landscape, anti-drone systems play a complementary role by reinforcing compliance and supporting enforcement mechanisms rather than replacing regulatory oversight.

At the operational level, the deployment of anti-drone technologies raises important considerations related to privacy, proportionality, and civil liberties. Effective security strategies must balance the need to protect critical infrastructure -such as airports- with the obligation to respect individual rights. Achieving this balance requires coordinated collaboration among regulatory authorities, airport operators, technology providers, and the broader civil community.

The discussion further emphasizes that the diversity and cultural specificity of operational contexts limit the effectiveness of singular or standardized security solutions. Airport environments vary significantly in terms of infrastructure, traffic density, and surrounding land use, requiring adaptive and context-sensitive approaches to counter-drone management. In densely populated areas, for example, the selection of detection and neutralization technologies must minimize collateral risks while maintaining operational effectiveness.

Finally, the successful integration of anti-drone systems depends not only on technological capabilities, but also on organizational preparedness. Personnel training, system interoperability, and the integration of human factors with technological systems are essential to ensuring effective aviation safety management. A holistic approach combining detection technologies, data analysis tools, and structured management systems supports a resilient and adaptive security posture tailored to the specific needs of each aerodrome.

In the specific context of Colombia, the discussion of anti-drone systems acqui-

res particular urgency given the country's unique security landscape. Unlike most nations where drone threats to civil aviation are primarily associated with reckless recreational use, Colombia faces the compounded challenge of organized armed groups systematically deploying unmanned aerial vehicles for surveillance, armed attacks, and logistics support to illicit activities.

The proliferation of low-cost commercial drones among violent non-state actors has been extensively documented in the academic literature: Chávez & Swed (2023) demonstrate that the tactical adoption of commercial UAV platforms by insurgent groups represents a structural shift in asymmetric warfare, reducing the technical and financial barriers that previously limited airpower to state actors. This dynamic is particularly salient in Colombia, where dissident factions of the Fuerzas Armadas Revolucionarias de Colombia (FARC) and the Ejército de Liberación Nacional (ELN) have progressively integrated drone capabilities into their operational arsenals.

According to the Presidencia de la República de Colombia (2025), a total of 115 drone-related incidents were recorded in 2024 alone, primarily perpetrated by illegal armed organizations and terrorist groups, targeting both security forces and critical infrastructure. Matiz-Rojas & Fernández-Camargo (2023) situate this phenomenon within the broader transformation of armed conflict in Colombia, highlighting the role of artificial intelligence and autonomous systems in reconfiguring the tactical environment for non-state actors. This figure represents a dramatic escalation compared to previous years and underscores the structural nature of the threat, consistent with global trends identified by Schwartz et al. (2022) in their cross-national analysis of armed drone proliferation and its implications for security governance. President Gustavo Petro publicly acknowledged in late 2025 that the conflict had evolved into a "war of drones and anti-drones," signaling the extent to which unmanned systems have reshaped the operational environment for national defense and aviation security alike (El Universo, 2026).

In response to this escalating threat, the Colombian government launched the Proyecto Escudo Nacional Antidrones (National Anti-Drone Shield Project), described by the Ministry of Defense as the most ambitious aerial defense strategy in the country's history (Segurilatam, 2026). With an initial budget of approximately USD 1.68 billion (COP 6.3 trillion), the project is structured around three foundational pillars: legislation and doctrine, training and operations, and technological deployment. Rather than constituting a simple procurement initiative, the Escudo Nacional represents a comprehensive framework that integrates detection networks based on radar and radio-frequency sensors, targeting the protection of critical infrastructure including energy facilities, governmental headquarters, and strategic military installations.

This multi-layered institutional approach aligns with recommendations in the counter-UAS literature, argue that effective anti-drone systems for facilities of national importance must be engineered around probabilistic detection models rather than single-technology deployments, a principle clearly reflected in the Colombian framework. The creation of a multidisciplinary drone and anti-drone unit comprising personnel from the armed forces and the National Police similarly resonates with findings by Okpaleke et al. (2023), who demonstrate in the context of West African counterinsurgency operations that cross-ins-

titutional drone coordination significantly improves both detection rates and operational response.

At the tactical level, Colombia has taken concrete steps toward deploying specific Counter-Unmanned Aircraft Systems (C-UAS) capabilities. The Ministry of Defense contracted the Dedrone Tracker AI C2 system developed by U.S.-based Dedrone Tactical at a cost of approximately USD 25.4 million, providing 360-degree spatial coverage with integrated electronic warfare capabilities for Army and Air Force installations across the country (Saumeth, 2025).

Simultaneously, regional authorities such as the Valle del Cauca and Cauca departmental governments have independently acquired ORION-10 MP and ORION-D MP systems from Singapore-based TRD Systems, incorporating both active inhibition and passive detection capabilities with a geolocation range of up to three kilometers (Webinfomil, 2024).

The decentralized nature of these acquisitions reflects the severity and geographic dispersion of drone-based threats across Colombian territory, a pattern consistent with what Mittal & Goetz (2025) describe as the "distributed threat" model characteristic of modern drone conflicts, in which adversaries exploit geographic breadth to overwhelm centralized defense architectures. Furthermore, the Fuerza Aeroespacial Colombiana (FAC) and the Corporación de Alta Tecnología para la Defensa (Codaltec) have jointly developed a domestic mobile anti-drone system capable of inhibiting GPS, GLONASS, and Wi-Fi signals. This development is significant not only operationally but also in terms of the emergence of national technological self-sufficiency in this domain, a capacity that Park et al. (2021) identify as a critical enabler of long-term counter-UAS governance for states facing persistent asymmetric drone threats.

On the regulatory front, Colombia has pursued parallel legislative efforts to accompany these technological investments. The Ministerio de Defensa, together with the Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) and the Ministerio de Transporte, introduced draft legislation before Congress to establish a comprehensive regulatory framework governing drone importation, registration, and operation, as well as the deployment of counter-drone systems. A key provision of this initiative designates MinTIC as the technical authority responsible for monitoring and blocking radio frequencies used by drones in illicit activities, including in airport zones and energy installations (Ministerio de Tecnologías de la Información y las Comunicaciones, 2025).

This approach to spectrum governance as a counter-drone instrument is consistent with the technical recommendations advanced by Popescu (2021) and later elaborated by Stastny & Stoica (2022), who identify radio-frequency management as a foundational layer of any national C-UAS framework for civil aviation. Additionally, Resolution 000242, enacted in January 2026, restricts UAV imports to designated entry points including El Dorado International Airport and the port of Cartagena, while prohibiting postal delivery as an import channel—a measure specifically designed to curtail smuggling of drones for criminal purposes (Dudenhoeffer, 2020; Dirección de Impuestos y Aduanas Nacionales, 2026). These regulatory developments demonstrate a growing recognition

that effective counter-drone governance requires the alignment of airspace regulation, spectrum management, and security policy within a unified national framework, a conclusion that resonates with Merkert & Bushell (2020) finding that regulatory fragmentation remains the primary structural barrier to effective UAS risk management across aviation systems.

Conclusions

The strategic management of unmanned aerial vehicles and anti-drone systems presents a growing challenge for civil aviation, particularly in the context of balancing technological innovation with regulatory control. This study highlights that the rapid expansion of drone operations both legal and illicit has exposed structural limitations within existing airspace management and security frameworks, especially in airport environments.

The findings support the conclusion that regulatory instruments alone are insufficient to address the risks associated with unregulated or malicious drone activities. Instead, an adaptive and proactive regulatory environment is required, supported by integrated management approaches that incorporate anti-drone systems within established aviation security protocols. Such integration should not rely on a single technological solution, but rather on a coordinated combination of detection, identification, and response systems tailored to the operational characteristics of each airport.

Furthermore, effective mitigation of drone-related threats depends on cross-sector collaboration involving governmental authorities, airport operators, industry stakeholders, and academic institutions. This collaborative approach is essential to anticipate emerging risks, address privacy and security concerns, and ensure the resilience of the civil aviation ecosystem.

Finally, the evolving nature of drone technologies and their potential misuse underscores the need for continued research and policy development. Future studies should further explore adaptive regulatory models, technological interoperability, and human factors within anti-drone and aviation safety management systems, contributing to a comprehensive and sustainable approach to safeguarding airport operations.

In the Colombian context, the conclusions of this study acquire additional dimensions that extend beyond the traditional scope of civil aviation security. The country presents a dual threat scenario in which drone misuse is simultaneously linked to airport operational disruptions and to active armed conflict involving illegal organizations. As documented by the Colombian Presidency (2025) and corroborated by regional security reports, the use of armed drones by dissident FARC factions and other non-state actors has inflicted significant human and material losses on the national armed forces, while also raising critical concerns regarding the security of civilian infrastructure including airports, energy facilities, and urban centers.

This phenomenon demonstrate that violent non-state groups increasingly exploit the affordability and versatility of commercial drone platforms to compensate for their conventional military inferiority, a trend that has accelerated sharply in Colombia since 2022. The

States facing higher levels of intrastate conflict and terrorism are significantly more likely to pursue and accelerate counter -drone programs- a pattern that Colombia's Proyecto Escudo Nacional clearly exemplifies. This dual threat profile demands that anti-drone strategies in Colombia be conceived not only within a civil aviation safety framework, but also as a component of national defense and public security policy, integrating civil-military coordination mechanisms.

The Proyecto Escudo Nacional Antidrones, launched in January 2026 with an initial investment of approximately USD 1.68 billion, represents the most significant institutional response to the drone threat in Colombian history and, according to available evidence, in the Latin American region as a whole. Structured around three pillars -legislation and doctrine, training and operations, and technological deployment- the initiative reflects the multi-dimensional approach advocated throughout this study and corroborated by comparative analyses of national counter-UAS programs.

The integration of electronic warfare capabilities with radar-based detection and AI-assisted command-and-control systems produces significantly higher threat neutralization rates than single-modal deployments—a finding with direct implications for the design of the Escudo Nacional. Its success will depend not only on the effective procurement and deployment of detection and neutralization systems, but on the simultaneous development of legal frameworks, institutional capacity, interoperability standards, and personnel training programs.

In this regard, regarding the organizational fragility of safety-security hybrid systems are particularly pertinent: the durability of the Escudo Nacional will require sustained investment in organizational learning and adaptive governance mechanisms beyond the initial technology procurement phase. The process of selecting technology providers through competitive evaluation involving more than 100 companies from 21 countries, with tests commencing in March 2026, is itself indicative of the complexity and strategic stakes involved.

From a civil aviation perspective, the conclusions of this study reinforce the urgency of extending anti-drone system integration to airport environments specifically. The Aeropuerto Internacional El Dorado, as the principal air hub of the country and a node for strategic infrastructure, has been the subject of prior technical studies proposing RF-based jamming systems capable of covering the full approach and landing area. These efforts, complemented by broader security technology upgrades including AI-assisted behavioral detection and high-definition monitoring systems implemented at El Dorado by the end of 2024, represent important advances but do not yet constitute a fully integrated counter-drone architecture.

This gap between incremental technological upgrades and systemic integration is precisely what identify as the central challenge for airports seeking to operationalize C-UAS capabilities: achieving functional coexistence between counter-drone systems and the electromagnetic environment of active airport operations remains technically demanding and institutionally complex. As this study concludes, such integration remains both a technical and institutional imperative for safeguarding the Colombian civil aviation ecosystem. Fu-

ture policy and research efforts should prioritize the harmonization of civil and defense anti-drone frameworks, ensuring that the protection of airport environments is explicitly addressed within the broader national aerial defense strategy an alignment that is achievable through the systematic expansion of Safety Management Systems to incorporate cybersecurity and counter-UAS dimensions as co-equal components of aviation security governance.

Mandatory Declaration on the Use of Generative AI

The authors declare that no generative artificial intelligence tools were used in the preparation of this manuscript.

References

Balladares, P., Bustos-Estrella, A., Albuja, G. & Alarcón, M. (2024). Advances in military drone technologies. *Athenea Engineering Sciences Journal, 5*(18), 7-18. https://doi.org/10.47460/athenea.v5i18.81

Bongiovanni, I. (2020). User safety and security experience: Innovation through design-inspired methods in airports in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 53-61). Springer. https://doi.org/10.1007/978-3-030-47229-0_6 PMid:32116208

Boyle, M. J. (2020). *The drone age: How drone technology will change war and peace.* Oxford Academic. https://doi.org/10.1093/oso/9780190635862.001.0001

Chávez, K. & Swed, O. (2021). The proliferation of drones to violent nonstate actors. *Defence Studies, 21*(1), 1-24. https://doi.org/10.1080/14702436.2020.1848426

Chávez, A. & Swed, O. (2023). Emulating underdogs: Tactical drones in the Russia-Ukraine war. *Contemporary Security Policy, 44*(4), 592-605. https://doi.org/10.1080/13523260.2023.2257964

Choi, Y. J. (2022). Security Threat Scenarios of Drones and Anti-Drone Technology. *Academy of Strategic Management Journal, 21*(1), 1-7. https://www.abacademies.org/abstract/security-threat-scenarios-of-drones-and-antidrone-technology-13612.html

Cole, M. (2014). Towards proactive airport security management: Supporting decision making through systematic threat scenario assessment. *Journal of Air Transport Management, 35*, 12-18. https://doi.org/10.1016/j.jairtraman.2013.11.002

Costin, A., Turtiainen, H., Khandker, S. & Hämäläinen, T. (2023). Towards a Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD) technologies and communications. *arXiv preprint arXiv:2302.08359.* https://doi.org/10.48550/arXiv.2302.08359 https://doi.org/10.14722/spacesec.2023.239280

Dirección de Impuestos y Aduanas Nacionales. (2 de febrero de 2026). *DIAN implementó nuevas medidas aduaneras para el control de la importación e ingreso de drones al país.* dian.gov.co. https://www.dian.gov.co/Prensa/Paginas/NG-DIAN-actualiza-disposiciones-y-fortalece-el-control-aduanero-para-el-ingreso-e-importacion-de-drones-al-pais.aspx

Dudenhoeffer, D. D. (2020). Day of the drone: Protecting critical infrastructure from terrorist use of unmanned aerial systems In A. Brill., K. Misheva. and M. Hadji-Janev (Eds.), *Toward effective cyber defense in accordance with the rules of law* (pp. 17-31). IOS Press. https://doi.org/10.3233/NHSDP200038

El Universo. (21 de enero de 2026). *El ambicioso escudo antidrones con el que Colombia quiere combatir las ofensivas aéreas de los grupos armados.* eluniverso.com. https://www.eluniverso.com/noticias/internacional/el-ambicioso-escudo-antidrones-con-el-que-colombia-quiere-combatir-las-ofensivas-aereas-de-los-grupos-armados-nota/

Hurtado-Cubillos, A. E. (2022). *Riesgos de las aeronaves remotamente tripuladas bajo el enfoque de ciberseguridad* [Tesis de especialización, Universidad Piloto de Colombia]. Repositorio institucional. http://repository.unipiloto.edu.co/handle/20.500.12277/12519

Hwang, S. P. & Kim, D. H. (2020). A study on the establishment of anti-drone system for the protection of national important facilities. *Journal of Digital Convergence, 18*(11), 247-257. https://doi.org/10.14400/JDC.2020.18.11.247

Jačionis, T. (2020). Modern methods for detection of unmanned aerial vehicles. *Mokslas Lietuvos ateitis / Science - Future of Lithuania, 12.* https://doi.org/10.3846/mla.2020.11435

Jore, S. H. (2020). Security and Safety Culture-Dual or Distinct Phenomena? in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 43-51). Springer. https://doi.org/10.1007/978-3-030-47229-0_5

Kang, D., Lee, G. & Choi, J. Y. (2021). Secure authentication protocol for drones in LTE networks [Conference paper]. *Advances in security, networks, and Internet of Things* (pp. 17-32). Springer, Cham. https://doi.org/10.1007/978-3-030-71017-0_2

La Cour-Harbo, A. & Schiøler, H. (2019). Probability of Low-Altitude Midair Collision Between General Aviation and Unmanned Aircraft. *Risk analysis: an official publication of the Society for Risk Analysis, 39*(11), 2499-2513. https://doi.org/10.1111/risa.13368 PMid:31291487 PMCid:PMC6899918

Law No. 12 of 1947. Whereby the Convention on International Civil Aviation, signed in Chicago on December 7, 1944, is hereby approved. November 7, 1947. D.O. No. 26537. https://www.cancilleria.gov.co/sites/default/files/Normograma/docs/arbol/1422.htm

Łukasiewicz, J. & Kobaszyńska-Twardowska, A. (2022). Proposed method for building an anti-drone system for the protection of facilities important for state security. *Security and Defence Quarterly, 39*(3), 88-107. https://doi.org/10.35467/sdq/149268

Mackie, T. & Lawrence, A. (2019). Integrating unmanned aircraft systems into airport operations: From buy-in to public safety. *Journal of Airport Management, 13*(4), 380-390. https://doi.org/10.69554/JJJB3489

Mantzana, V., Georgiou, E., Chasiotis, I., Gkotsis, I., Stelkens-Kobsch, T. H., Kazoukas, V., Papagiannopoulos, N., Nikas, A. & Komninos, F. (2020). Airports' crisis management processes and stakeholders involved. *Annals of Disaster Risk Sciences, 3*(1). https://doi.org/10.51381/adrs.v3i1.47

Matiz-Rojas, A. H. & Fernández-Camargo, J. A. (2023). On the use of artificial intelli -gence as a means and methods in armed conflicts. *Revista Científica General José María Córdova, 21*(42), 525-549. https://doi.org/10.21830/19006586.1151

Merkert, R. & Bushell, J. (2020). Managing the drone revolution: A systematic literature review into the current use of airborne drones and future strategic directions for their effective control. *Journal of Air Transport Management, 89*, 101929. https://doi.org/10.1016/j.jairtraman.2020.101929 PMid:32952321 PMCid:PMC7489224

Ministerio de Tecnologías de la Información y las Comunicaciones. (30 de julio de 2025). *Ministerios TIC y de Defensa radican proyecto de Ley para regular el uso de drones en el país.* mintic.gov.co. https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/404027:Ministerios-TIC-y-de-Defensa-radican-proyecto-de-Ley-para-regular-el-uso-de-drones-en-el-pais

Mittal, V. & Goetz, J. (2025). A quantitative analysis of the effects of drone and counter-drone systems on the Russia-Ukraine battlefield. *Defense & Security Analysis, 41*(3), 490-503. https://doi.org/10.1080/14751798.2025.2479973

Niño-Rojas, V. M. (2011). *Metodología de la investigación: Diseño y ejecución.* Ediciones de la U.

Okpaleke, F. N., Nwosu, B. U., Okoli, C. R. & Olumba, E. E. (2023). The case for drones in counter-insurgency operations in West African Sahel. *African Security Review, 32*(4), 351-367. https://doi.org/10.1080/10246029.2023.2217158

Öz, T. & Sert, S. (2019). The present role of anti-drone technologies in modern warfare and projected developments. *Güvenlik Stratejileri Dergisi, 15*(32), 691-711. https://doi.org/10.17752/guvenlikstrtj.668216

Park, S., Kim, H. T., Lee, S., Joo, H. & Kim, H. (2021). Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access, 9*, 42635-42659. https://doi.org/10.1109/ACCESS.2021.3065926

Pérez-Herrera, P. G. (2013). Estudio y simulación de un sistema de vigilancia aeronáutica para el control de aproximación de aeronaves a el aeropuerto El Dorado, basado en la tecnología MLAT (Multilateración). *Redes de Ingeniería, 4*(1), 85-94. https://doi.org/10.14483/2248762X.6426

Pettersen-Gould, K. & Bieder, C. (2020). Safety and security: The challenges of bringing them together in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 1-8). Springer. https://doi.org/10.1007/978-3-030-47229-0_1

Popescu, L. R. (2021). The existing technologies on anti-drone systems. [Paper presentation]. *International Conference on Knowledge-Based Organization,* Volume 27, Issue 3, 83-91. https://doi.org/10.2478/kbo-2021-0093

Presidencia de la República de Colombia. (8 de enero de 2025). *Colombia fortalece seguridad nacional con plan anti-drones para contrarrestar amenazas y proteger infraestructuras estratégicas.* Presidencia.gov.co. https://www.presidencia.gov.co/prensa/Paginas/Colombia-fortalece-seguridad-nacional-con-plan-anti-drones-para-contrarrest-250108.aspx#:~:text=Bogot%C3%A1%2C%208%20de%20enero%20de,de%20energ%C3%ADa%20y%20centros%20poblados

Saumeth, E. (3 de junio de 2025). *Colombia adquiere sistemas antidron por 25 millones de dólares.* Infodefensa.com. https://www.infodefensa.com/texto-diario/mostrar/5312190/074-colombia-colombia-adquiere-sistemas-anti-dron-25-millones-dolares

Schulman, P. R. (2020). Safety and security: Managerial tensions and synergies in C. Bieder y K. Pettersen-Gould (eds), *The coupling of safety and security: Exploring interrelations in theory and practice* (pp. 87-95). Springer. https://doi.org/10.1007/978-3-030-47229-0_9

Schwartz, J. A., Fuhrmann, M. & Horowitz, M. C. (2022). Do Armed Drones Counter Terrorism, Or Are They Counterproductive? Evidence from Eighteen Countries. *International Studies Quarterly, 66(*3), sqac047, https://doi.org/10.1093/isq/sqac047

Segurilatam. (23 de enero de 2026). *¿En qué consiste el Proyecto Escudo Nacional Antidrones de Colombia?* Segurilatam.com. https://www.segurilatam.com/actualidad/proyecto-escudo-nacional-antidrones-de-colombia_20260123.html

Semenyuk, V., Kurmashev, I., Lupidi, A., Alyoshin, D., Kurmasheva, L. & Cantelli-Forti, A. (2025). Advances in UAV detection: integrating multi-sensor systems and AI for enhanced accuracy and efficiency. *International Journal of Critical Infrastructure Protection, 49*, 100744. https://doi.org/10.1016/j.ijcip.2025.100744

Shin, J. M., Kim, Y. S., Ban, T. W., Choi, S., Kang, K. M. & Ryu, J. Y. (2021). Position tracking techniques using multiple receivers for anti-drone systems. *Sensors, 21*(1),

35. https://doi.org/10.3390/s21010035 PMid:33374686 PMCid:PMC7793488

Shvetsova, S. V. & Shvetsov, A. V. (2021). Ensuring safety and security in employing drones at airports. *Journal of Transportation Security, 14,* 41-53. https://doi.org/10.1007/s12198-020-00225-z

Sichko, P. (2019). Integrating unmanned aerial system operations into the Dallas/Fort Worth airport environment. *Journal of Airport Management, 13*(3), 206-214. https://doi.org/10.69554/CMDK2637

Stastny, P. & Stoica, A. M. (2022). *Protecting aviation safety against cybersecurity threats* [Paper presentation]. IOP Conference Series: Materials Science and Engineering, Volume 1226(1), 012025, Salerno. https://doi.org/10.1088/1757-899X/1226/1/012025

Tezza, D. & Andujar, M. (2019). The state-of-the-art of human–drone interaction: A survey. *IEEE Access, 7*, 167438-167454. https://doi.org/10.1109/ACCESS.2019.2953900

Unidad Administrativa Especial de Aeronáutica Civil de Colombia. (2023). *Action plan of the Unmanned Aviation Strategic Plan 2023-2026*. https://www.aerocivil.gov.co/autoridad_aeronautica/publicaciones/3958/aviacion-no-tripulada-uasdrones/

Webinfomil. (13 de septiembre de 2024). *El Ejército de Colombia recibió sistemas antidrones ORION-10 MP y ORION-D MP.* Webinfomil.com. https://www.webinfomil.com/2024/09/el-ejercito-de-colombia-recibio.html

Završnik, A. (2016). Introduction: Situating Drones in Surveillance Societies in A. Završnik (Ed.), *Drones and unmanned aerial systems* (pp. 1-18). Springer. https://doi.org/10.1007/978-3-319-23760-2_1

Revista Perspectivas en Inteligencia
(Scientific Journal of Social Sciences and Interdisciplinary Studies)
Volume 18, Number 27, January - June 2026
ISSN: 2145-194X (printed), 2745-1690 (online)
Website: https://revistaseditorialejc.org/index.php/pei
Bogotá D.C., Colombia

Anti-Drone Systems for Aviation Security in the Colombian Civil Aviation Ecosystem

Disclosure Statement
The authors declare that there are no potential conflicts of interest related to this article.

Funding
The authors do not report any source of funding for the preparation of this article.

About the author(s)
Oscar Alberto Rojas-Martínez Master's Degree in Education from the Nueva Granada Military University (Colombia), with a specialization in Aeronautical and Aerospace Administration from the Nueva Granada Military University (Colombia), a degree in Business Administration from the Nueva Granada Military University (Colombia), and a degree in Military Sciences from the Escuela Militar de Cadetes General José María Córdova (Colombia), he is a university professor and researcher in the areas of aviation operational safety, higher education, human factors, security, and defense.

https://orcid.org/0000-0002-3826-2706 - Contact: nacho_rojas07@hotmail.com

Heivar Yesid Rodríguez-Pinzón Ph.D. candidate in Management Administration at Benito Juárez University (Mexico), holds a Master's degree in Economic Sciences from Santo Tomás University (Colombia) and a degree in Statistics from the National University (Colombia), he is a university professor and scientific researcher specializing in time-series and econometric models.

https://orcid.org/0000-0002-9553-0455 - Contact: rodriguezphy@javeriana.edu.co