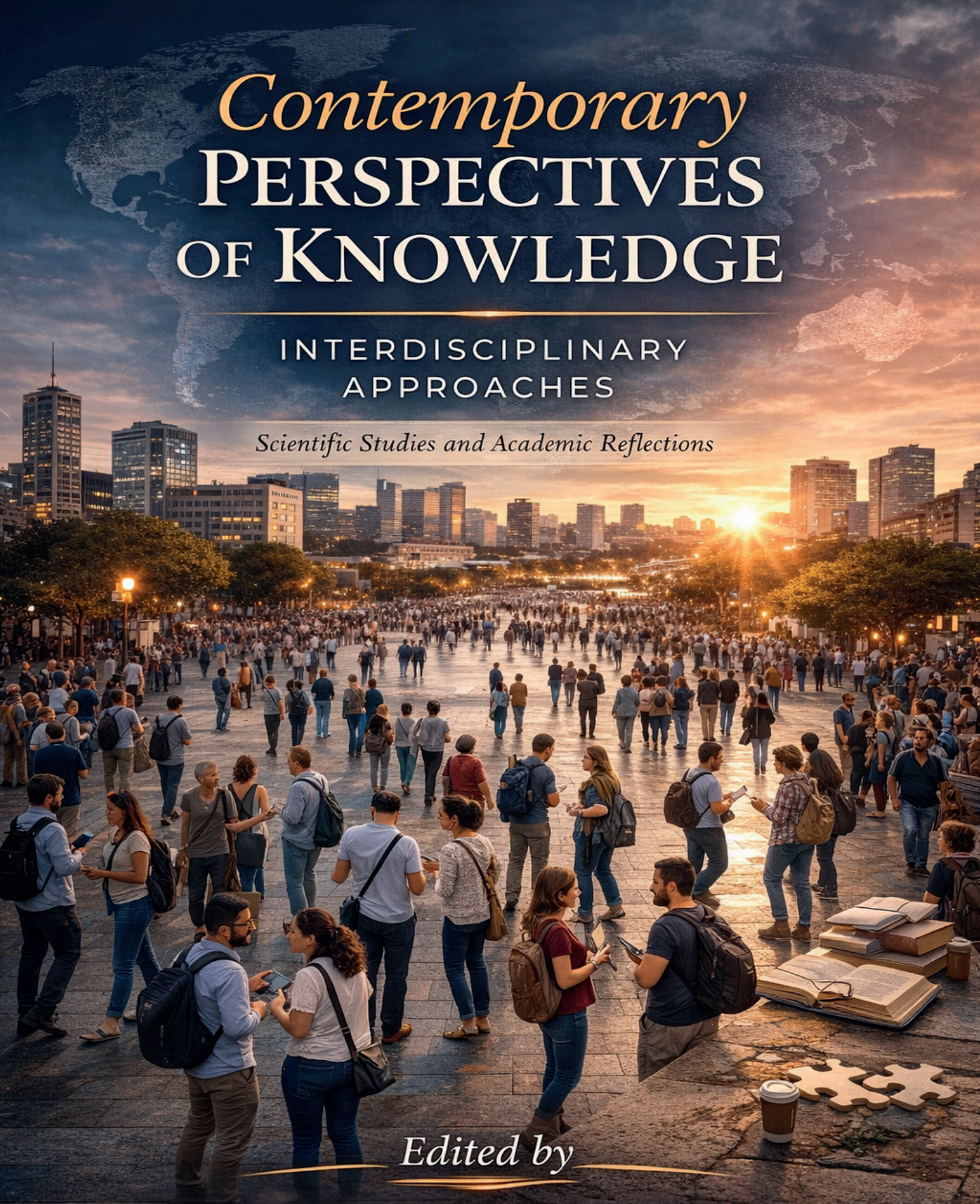
Contemporary PERSPECTIVES OF KNOWLEDGE

INTERDISCIPLINARY APPROACHES

Scientific Studies and Academic Reflections



Edited by

Flávia Moreno Alves de Souza

Periodicojs
EDITORA ACADÊMICA

Editorial Team

Abas Rezaey

Ana Maria Brandão

Fernado Ribeiro Bessa

Filipe Lins dos Santos

Flor de María Sánchez Aguirre

Isabel Menacho Vargas

Izabel Ferreira de Miranda

Leides Barroso Azevedo Moura

Luiz Fernando Bessa

Manuel Carlos Silva

Renísia Cristina Garcia Filice

Rosana Boullosa

Graphic Design, Layout and Cover

Academic Publisher Periodicojs

Language

Portuguese and English

International Cataloging-in-Publication Data (CIP)

(Brazilian Book Chamber, SP, Brazil)

C761 Contemporary Perspectives of Knowledge: Interdisciplinary Approaches/ Flávia Moreno Alves de Souza (org) – João Pessoa: Periodicojs publisher, 2026.

E-book: il. color.

Includes bibliography
ISBN: 978-65-6010-196-8

1. Free themes. I. Souza, Flávia Moreno Alves. II. Title

CDD 370

Prepared by Dayse de França Barbosa CRB 15-553

Index for systematic catalog:

Indexes for systematic catalog:

1. Education: 370

Work without funding from public or private bodies.

The published works have been submitted to peer review and evaluation (double-blind), with respective acceptance letters in the publisher's system.

The work is the result of studies and research from the Interdisciplinary Studies in Human Sciences section of the Humanities in Perspective book collection.



Filipe Lins dos Santos
President and Senior Editor of Periodicojs

CNPJ: 39.865.437/0001-23

Rua Josias Lopes Braga, n. 437, Bancários, João Pessoa - PB - Brazil
website: www.periodicojs.com.br
instagram: @periodicojs

38 DRONES IN PUBLIC AND PRIVATE SECURITY: TECHNOLOGICAL CAPABILITY, REGULATION, AND HUMAN COMPETENCE UNDER THE NEW ICA 100-40

Chapter



DRONES IN PUBLIC AND PRIVATE SECURITY: TECHNOLOGICAL CAPABILITY, REGULATION, AND HUMAN COMPETENCE UNDER THE NEW ICA 100-40

Francisco Celso de Lima Machado[1]

Abstract: Remotely piloted aircraft—popularly known as drones—are no longer a technological promise; they have become operational infrastructure for public and private security. Drawing on recent high-impact literature, this chapter takes a technical and scientific look at how these platforms are being integrated into policing, search and rescue, forensic investigation, surveillance, and asset protection. Its regulatory anchor is the new edition of Brazilian Air Force Command Instruction ICA 100-40, issued by the Department of Airspace Control (DECEA) and in force as of July 1, 2026 (BRASIL, 2026). The analysis brings together three inseparable dimensions: the technological, the regulatory, and the human. Throughout, the chapter advances one central thesis: the effectiveness of these operations is not decided by the equipment, but by the architecture of competence, risk governance, and compliance that surrounds it. It examines the defining tension between operational effectiveness and the protection of fundamental rights—above all privacy and public acceptance—and presents, as a case study, the experience of the Pará State Public Security and Social Defense System (SIEDS) and its Public Security Air Group (GRAESP) in a biome of exceptional operational complexity. The chapter concludes that the ongoing regulatory transition demands from managers a competence that goes well beyond piloting skills: the ability to make decisions under uncertainty while bearing full legal and operational responsibility for them.

Keywords: remotely piloted aircraft; public security; private security; ICA 100-40; risk management; public acceptance

[1] Military Firefighter, Specialization in Strategic Management in Public Security from the Pará Institute of Security Education - IESP

INTRODUCTION

Little more than a decade ago, a remotely piloted aircraft at a security operation was a noteworthy exception; today, it is simply assumed to be part of the deployment. This shift—from novelty to infrastructure—has outpaced the ability of institutions to absorb it, opening a gap that shows up on three fronts at once: the technological front, where equipment capabilities evolve faster than the protocols meant to govern them; the regulatory front, where rules chase, with some delay, a rapidly changing operational reality; and the human front, where the training of operators—and, above all, of managers—has not kept pace with adoption. This chapter focuses on that gap and argues that closing it is not primarily a matter of buying equipment, but of building institutional competence.

The term drone, although firmly established in everyday usage, is not the technical-legal term used in Brazilian regulation. In Special Brazilian Civil Aviation Regulation RBAC-E No. 94, the National Civil Aviation Agency (ANAC) distinguishes, by purpose, between model aircraft—used for recreation—and remotely piloted aircraft (RPA), used for commercial, institutional, or experimental purposes (BRASIL, 2017). The aircraft, its remote pilot station, its command-and-control links, and its other components together make up the Remotely Piloted Aircraft System (RPAS). These terms are used here with the precision each context requires.

The literature bears out the importance of the topic. Police forces in many countries are increasingly adopting drones because they help officers detect risks and respond to incidents with timely, low-cost services (CHEN et al., 2023). Their spread, however, is not socially neutral: a systematic review of thirty acceptance surveys conducted in fifteen countries shows that without broad public approval, drones will never live up to their considerable potential, and that perceived benefits and risks are what ultimately determine their acceptance (SABINO et al., 2022). The choice of ICA 100-40 as the chapter's anchor is deliberate. Issued by DECEA through Ordinance No. 2094/DNOR8 of March 18, 2026, and in force as of July 1, 2026, it consolidates into a single document the rules governing access

to Brazilian airspace by unmanned aircraft—precisely at the moment operational adoption is reaching maturity (BRASIL, 2026). The chapter then moves through the technological foundations of these platforms, the regulatory framework, public and private applications, privacy and acceptance issues, the adversarial side of the technology, and the human factor, before closing with a case study and final remarks.

The chapter aims to make three contributions. First, it brings the public and private applications of drones—currently treated in fragmented fashion—under a single analytical framework, showing that they share the same technological base and, in Brazil, the same regulatory architecture. Second, it grounds the discussion in recent high-impact literature, moving beyond the merely descriptive or promotional tone that dominates applied debate. Third, and most important, it shifts the focus of analysis from equipment to competence, demonstrating that the difference between owning a platform and actually producing security lies in the human and institutional architecture that operates and governs it.

TECHNOLOGICAL FOUNDATIONS: WHAT THE PLATFORM ACTUALLY DOES

Understanding how drones are applied to security requires understanding what these platforms technically do. The term force multiplier captures the core idea: a drone lets a team perform, with fewer resources and less exposure to risk, tasks that once required large numbers of personnel, expensive crewed aircraft, or physical exposure to dangerous environments. This multiplication of capability, however, breaks down into specific sets of functions, and mastering them is a precondition for effective operations.

The core of a drone's operational value is its sensing capability. High-resolution optical cameras with long-range zoom allow detailed observation from distances that keep an operation covert—a decisive attribute in intelligence work. The real leap, however, comes from thermal sensing: thermal cameras detect the infrared radiation emitted by any object above absolute zero, making observation independent of visible light and enabling operations at night, through smoke and fog, or beneath the forest canopy. In search and rescue, this property is decisive, because it makes it possible to locate people by their heat signature

against cooler backgrounds—a capability that is the subject of active research on thermal image tracking for rescue missions (YEOM, 2024) and on AI-assisted human rescue in disaster environments (PAPYAN et al., 2024).

The second decisive dimension is the range regime, which regulators classify according to the relationship between the remote pilot and the aircraft. In visual line of sight (VLOS) operations, the pilot maintains direct visual contact; in extended visual line of sight (EVLOS) operations, the pilot relies on visual observers; and in beyond visual line of sight (BVLOS) operations, visual contact cannot be maintained even through observers (BRASIL, 2017). BVLOS is the technological and regulatory frontier of security applications, because it enables patrols along long stretches of border, monitoring of vast areas of forest or coastline, and response to incidents far from base—at the cost of requiring the most robust detect-and-avoid systems, resilient links, and contingency procedures. Flight endurance, typically between twenty-five and forty-five minutes for platforms carrying thermal cameras, imposes concrete constraints that planning must anticipate; these are mitigated by drone-in-a-box solutions, which allow autonomous takeoff, landing, and recharging from fixed docking stations.

THE BRAZILIAN REGULATORY FRAMEWORK

A common mistake in institutional adoption is to treat the drone as a stand-alone piece of equipment, when it is in fact a node in a complex system: the data captured by the sensor must be transmitted securely, processed, integrated with other sources, and turned into a product that supports decision-making. The diversity of platforms—compact multirotors for urban operations and confined spaces; hexacopters for heavier payloads and longer missions; fixed-wing and vertical takeoff and landing (VTOL) aircraft for greater range and endurance—confirms that procurement decisions should start from the mission, not from the equipment. The payload, after all, is what turns the platform into a tool: the same airframe can serve forensics, rescue, or intelligence depending on the sensor it carries.

The third technical dimension—often underestimated—is connectivity. The

command-and-control link, through which the pilot flies the aircraft, and the data link, through which imagery and telemetry return to the ground station, are critical points of failure whose robustness determines whether an operation is viable, especially beyond visual line of sight. The expansion of BVLOS operations depends heavily on resilient connectivity, often achieved by combining multiple redundant channels so that losing one link does not mean losing the aircraft; contingency procedures—automatic return to home, safe landing at pre-designated sites—are therefore a requirement for any professional operation. This dependence ties the technical dimension to cybersecurity: the specialized literature shows that the growing connectivity and autonomy of these platforms expand their attack surface, making data integrity and resistance to interception and control hijacking critical requirements—neglect them, and a security asset can become a vulnerability (CHAMOLA et al., 2021).

THE BRAZILIAN REGULATORY FRAMEWORK

Unmanned aircraft operations in Brazil are subject to an architecture built on three institutional pillars, and understanding it is a prerequisite for any lawful operation. ANAC regulates civil aviation, including airworthiness, aircraft registration, and operator certification. DECEA manages the airspace, setting access rules, altitudes, and restricted zones. The National Telecommunications Agency (ANATEL) regulates the radio frequencies used for command and control. Compliance requires observing all three domains at once; neglecting any one of them undermines the legality of the operation and exposes the operator to administrative, civil, and criminal penalties.

On the ANAC side, the rule in force is RBAC-E No. 94, issued in 2017 and updated in 2023, which classifies operations by visual range and imposes conditions such as a minimum distance of thirty meters (about 100 feet) from non-consenting persons, a limit of one aircraft per pilot, and registration of drones weighing more than 250 grams (about 0.55 lb) in the Unmanned Aircraft System registry (SISANT) (BRASIL, 2017). A broader transition is under way: the proposed RBAC 100, submitted to Public Consultation No. 09/2025, seeks to

adopt the European risk-based model, with Open, Specific, and Certified categories, in line with the guidelines of the International Civil Aviation Organization and the European Union Aviation Safety Agency (BRASIL, 2025). Until it is actually enacted, however, RBAC-E No. 94 remains the enforceable rule.

On the DECEA side, the centerpiece is ICA 100-40, whose new edition introduces changes with direct impact (BRASIL, 2026). The first and most significant is that prior authorization is now required for all unmanned aircraft, regardless of weight: equipment weighing up to 250 grams, which previously enjoyed differentiated treatment, now requires access authorization through the SARPAS system. This universal requirement eliminates an operational gray area and has significant consequences for private security. The second change is the reduction, from twelve to eight calendar days, of the minimum lead time for requesting operations that require segregated airspace, which gives planners more flexibility. A common misconception, however, must be cleared up: ICA 100-40 does not automatically clear urgent operations, nor does it waive prior authorization on grounds of urgency. What it does is consolidate and streamline procedures, shorten lead times, and unify rules. Operational urgency is accommodated through coordination with air traffic control authorities, not by suspending safety requirements.

This regulatory consolidation has an effect that goes beyond its specific provisions: it raises the bar for compliance and makes ignorance of the rules harder to defend. The literature shows, however, that issuing rules is not enough. A study of unmanned aircraft users' compliance with civil aviation rules reveals that actual compliance depends on factors beyond the regulatory text itself, such as operators' knowledge of the rules and their perception of the rules' legitimacy (HENDERSON; SHELLEY, 2023). For public and private institutions, this means that drone operations are leaving the realm of tolerated improvisation and entering that of auditable compliance—a transition whose success depends less on the rule itself than on the competence of those who apply it.

APPLICATIONS IN PUBLIC SECURITY

Drone applications in public security span a spectrum that runs from emergency response to criminal investigation, and they all share one common trait: they turn the drone into a tool for informational advantage, giving decision-makers an understanding of the scene earlier, and in greater depth, than conventional means allow.

TACTICAL RESPONSE AND THE RISK-BASED PARADIGM

The model that best captures this logic is Drone as First Responder (DFR): when a call comes in, a camera-equipped aircraft is launched to reach the scene first, giving responding officers a view of the location before they arrive. Officer safety is a recurring benefit, since the platform allows the risk at a scene to be assessed before officers are physically exposed. Recent research has shifted the planning of this use toward a risk-based approach. A framework for optimizing police drone deployment based on street-level crime risk, validated with real data from a city, shows how distance metrics and optimal base locations can be calibrated to risk while explicitly incorporating constraints such as residential privacy and flight altitude; it proposes moving drone policing toward a risk-driven logic (CHEN et al., 2023). This approach is instructive because it combines, in a single decision model, operational effectiveness and the containment of risk to third parties—precisely the synthesis a mature operation requires.

The tactical value of this use shows up in measurable gains in time and safety. Early information allows officers to understand the nature and severity of an incident before reaching the scene, so they can size the response and resources appropriately, reducing both officers' exposure and the risk to bystanders. The literature on optimal placement of these platforms shows that the choice of distance metrics and base locations directly affects the capacity for timely response—so it is planning, and not merely the availability of equipment, that turns technology into operational performance (CHEN et al., 2023). This shift in focus, from owning the platform to using it intelligently, is consistent with the central thesis of this

chapter.

SEARCH AND RESCUE

There is one domain in which the value of drones is less contested and more immediately humanitarian: search and rescue. By combining rapid coverage of large areas with the detection of heat signatures, the platform directly affects the odds of survival, while simultaneously overcoming the three limitations of traditional methods—the slowness of ground searches, the dependence of crewed air searches on daylight and weather, and the high cost of the latter. Research continually validates and refines these capabilities, from thermal tracking to locate people (YEOM, 2024) to AI-assisted rescue in disaster scenarios (PAPYAN et al., 2024). Field forensics benefits as well: a systematic review of nineteen studies on drone-based remote sensing for locating human remains and clandestine graves confirms that optical, thermal, and multispectral sensors offer a non-invasive, low-cost alternative, while cautioning that methodological fragmentation and inconsistent reporting of flight parameters still limit the forensic robustness of these methods (DE BRUYN et al., 2025). Public acceptance tracks this usefulness: research on public acceptance of beach-rescue drones shows that protection and rescue applications are among those the public approves of most (DEL-REAL; DÍAZ-FERNÁNDEZ, 2021)—a finding that matters for the institutional sustainability of drone use. In the Amazon context, with its archipelagos, long beaches, and hard-to-navigate rivers, this capability takes on special importance.

AERIAL FORENSICS AND FORENSIC PHOTOGRAMMETRY

Scene documentation is a third high-value front. Traditional crime scene photography has significant limitations at complex outdoor scenes, where a ground-level perspective is not enough to capture spatial relationships. Drones provide comprehensive aerial documentation, and photogrammetry—metric three-dimensional reconstruction from overlapping images—takes this record further, producing orthomosaics and 3D models that

can be measured, annotated, and re-examined after the scene has been released. At large or hard-to-reach scenes, three-dimensional orthophotography gives the forensic examiner a verifiable metric record, improves the accuracy of the expert report, reduces reliance on error-prone manual measurements, and shortens the time teams spend on site, with gains in both safety and efficiency. Integrated with other forensic sources, aerial documentation creates a record that all parties to a case can re-examine, strengthening the adversarial process and the robustness of technical evidence.

INTELLIGENCE, ENVIRONMENTAL MONITORING, AND RIVER OPERATIONS

The fourth front is intelligence and surveillance. Long-range zoom, combined with the discretion that distance provides, makes it possible to monitor targets—clandestine ports, narrow river channels, illegal gold-mining sites—without revealing the team's presence, preserving the informational edge that is the essence of intelligence work. In the fight against environmental crime, drones have been used to identify degraded areas, monitor deforestation, and detect illegal mining—fronts on which the ability to quickly cover vast stretches of forest and coastline is decisive. The experience in Pará illustrates how these fronts come together: the operator training conducted by the Air Group in partnership with the River Group was designed to expand operations in hard-to-reach areas, monitor rivers and forests, and combat environmental crimes and other illicit activities. The riverine and forested character of the Amazon turns the drone from a convenience into an operational necessity, and coordination between the air and river groups into a condition for effectiveness. The same capability supports the policing of large events by giving command centers a real-time aerial view of crowds—a use that, however, sharply reintroduces the privacy and civil liberties tensions discussed below. In major-event policing, the ability to obtain a real-time panoramic aerial view of crowds, combined with zoom that makes physical approach unnecessary, makes the drone a prime tool for coordinating deployments at stadiums, demonstrations, and mass gatherings, with a related application in traffic management, where it informs decisions on traffic flows and detours. It is also, however, the arena in which civil liberties tensions are

most acute: aerial monitoring of assemblies raises concerns about a chilling effect on the exercise of the right of assembly. Proportionality of use, transparency about purpose, and respect for constitutional limits are therefore conditions not only for the legality but also for the democratic legitimacy of the operation—a requirement consistent with the finding that public acceptance varies with perceived purpose and with trust in institutions (SABINO et al., 2022).

APPLICATIONS IN PRIVATE SECURITY

The migration of the technology from the public to the private domain has followed a logic of capability transfer: the same properties that make it valuable for policing—persistent surveillance, wide-area coverage, thermal sensing, and reduced human exposure—address the structural needs of asset protection and corporate security.

PERIMETER SURVEILLANCE AND CRITICAL INFRASTRUCTURE PROTECTION

The most widespread application is perimeter surveillance. Airports, power plants, data centers, industrial complexes, refineries, ports, and logistics facilities are critical assets whose long perimeters challenge traditional patrols. Drones make it possible to run aerial perimeter checks, sweep for intrusions, and use thermal cameras to spot anomalous activity, ensuring that vulnerabilities are detected before they become threats. They can be programmed to patrol predefined routes autonomously and act as a force multiplier for security teams, especially where ground patrols are resource-intensive or unable to respond quickly. Integration with artificial intelligence—autonomous monitoring with real-time detection and analysis—is the defining trend in this segment. Yet the very centrality of drones to critical infrastructure protection is double-edged: the literature warns that unmanned aircraft also threaten critical energy infrastructure, requiring dedicated defense strategies (KOOTALA; MOUSA; PONG, 2023)—a topic revisited in the section on the adversarial side.

The strategic importance of the private segment is underscored by its rapid growth and by its technological convergence with the public sector. Protecting energy facilities, oil and gas complexes, ports, and transportation hubs—exposed to threats ranging from espionage to sabotage—finds in perimeter surveillance drones an agile and versatile ally for early detection. Integration with video analytics and autonomous detection, however, shifts part of the decision-making from the human operator to the system, which brings the governance requirements discussed below into the private sector as well: detection reliability, false-alarm management, and human oversight of automated responses become conditions for any operation that aims to be both effective and legally defensible.

TETHERED DRONES AND THE PUBLIC–PRIVATE BOUNDARY

One specific solution deserves attention: the tethered drone, connected to its ground station by a cable that supplies continuous power and a secure data link. By giving up wide-ranging mobility, it solves the main limitation of aerial surveillance—battery endurance—allowing extended loitering over a fixed point, with less exposure to interference and lower risk of flyaways. The expansion of drone-based private security, however, raises a boundary question. Unlike public operators, who hold legal authority and are subject to institutional oversight, private operators act under ordinary law, with narrower limits on capturing images of third parties and on surveilling other people's property. What is legitimate policing for the state may, for a private party, amount to unlawful surveillance if it spills beyond the perimeter that is legitimately being protected. In the private sector, compliance with Brazil's General Data Protection Law (LGPD) (BRASIL, 2018), respect for others' property, and observance of aeronautical distance and authorization rules are not only legal requirements but conditions for the sustainability of the business itself.

PRIVACY, PUBLIC ACCEPTANCE, AND GOVERNANCE

One specific solution deserves attention: the tethered drone, connected to its ground

station by a cable that supplies continuous power and a secure data link. By giving up wide-ranging mobility, it solves the main limitation of aerial surveillance—battery endurance—allowing extended loitering over a fixed point, with less exposure to interference and lower risk of flyaways. The expansion of drone-based private security, however, raises a boundary question. Unlike public operators, who hold legal authority and are subject to institutional oversight, private operators act under ordinary law, with narrower limits on capturing images of third parties and on surveilling other people's property. What is legitimate policing for the state may, for a private party, amount to unlawful surveillance if it spills beyond the perimeter that is legitimately being protected. In the private sector, compliance with Brazil's General Data Protection Law (LGPD) (BRASIL, 2018), respect for others' property, and observance of aeronautical distance and authorization rules are not only legal requirements but conditions for the sustainability of the business itself.

The technical ability to observe is not the same as the legal authority to do so. This is the point of greatest tension in the use of drones for security, and recent literature addresses it systematically. The review of thirty acceptance surveys conducted in fifteen countries concludes that the public tends to see drones as a technology that directly intrudes on their privacy, and that public approval varies dramatically by purpose—high for public safety and research uses, low for commercial uses—with perceived benefits and risks, rather than mere exposure to the technology, determining acceptance (SABINO et al., 2022). In this literature, trust emerges as the central variable, and transparency as the main mechanism for building it.

In the Brazilian context, the balance between effectiveness and rights is structured by the General Data Protection Law (BRASIL, 2018) and by the constitutional guarantees of privacy and the inviolability of the home, which impose concrete limits on the capture, storage, and processing of images. The literature is particularly attentive to the risk of disproportionate use and to the potential chilling effect on the right of assembly when aerial monitoring targets demonstrations and gatherings. The most promising response is not to give up the technology, but to embed it in a risk-based regime: by internalizing residential privacy and altitude as explicit constraints of the deployment model, the risk-driven optimization framework (CHEN et al., 2023) offers a concrete example of how the protection of rights can

be built into the engineering of the operation itself, rather than treated as an external limit. The lesson for managers is clear: public acceptance, a condition for institutional sustainability, depends on transparency, proportionality, and accountability—not just on operational effectiveness.

The international landscape sheds light on the possible paths for this kind of governance. In jurisdictions that have widely rolled out Drone as First Responder programs, documented operational gains have coexisted with an organized backlash from civil liberties advocates, who question the opacity of usage data and the risk of disproportionate surveillance of vulnerable communities. The European regulatory model, which is risk-based and organized into operational categories according to the magnitude of risk, seeks to calibrate regulatory requirements to the concrete hazard of each flight—an approach that inspires the Brazilian RBAC 100 proposal (BRASIL, 2025) and that aligns with evidence that regulatory compliance depends on operators' perception of legitimacy (HENDERSON; SHELLEY, 2023). The overarching lesson is that no jurisdiction has fully resolved the tension between effectiveness and rights; what sets the most mature experiences apart is the institutionalization of mechanisms for transparency, proportionality, and accountability.

THE ADVERSARIAL SIDE: HOSTILE THREATS, COUNTER-UAS, AND DRONE FORENSICS

An honest analysis must acknowledge that the same technology that protects can also threaten. The growing accessibility and capability of these platforms have enabled their use in illicit activities—smuggling, unauthorized surveillance, delivery of prohibited items, and cyberattacks. In correctional facilities, drone overflights to drop contraband have become a concrete operational problem, to which Pará responded with dedicated operator training by its corrections administration, in coordination with the air and river groups. Counter-drone defense—counter-UAS—thus emerges as the mirror image of adoption itself, made up of three linked functions: detection, identification, and mitigation. The technical literature has systematized this field: a comprehensive review of attacks on unmanned aerial vehicles and of

neutralization techniques maps the platforms' vulnerabilities and the range of countermeasures, showing that each function raises its own technical and legal challenges (CHAMOLA et al., 2021). Neutralizing an aircraft in flight, in particular, involves risks to third parties and legal limits that only state operators, in specific circumstances, may legitimately cross.

This scenario explains the importance of drone forensics, understood as the systematic examination of an aircraft to extract and analyze digital data capable of revealing its activities, its operators, and its purposes. The consolidation of this discipline faces a recognized obstacle: despite numerous technical studies, there is still no comprehensive, standardized investigative framework—a gap that recent research seeks to fill through conceptual investigation models applicable to the field (AL-DHAQM et al., 2021). Reconstructing flight paths from the satellite navigation data of aircraft from mainstream manufacturers is now an established forensic technique (KUMAR; AGRAWAL, 2021), and the distinction between static and live acquisition of digital evidence is a central methodological challenge for forensic traceability (SALAMH et al., 2021). For security institutions, the implication is that drone competence does not end with offensive and defensive operations; it extends to the investigative capacity to process a seized aircraft as a source of evidence—an examination that requires a rigorous chain of custody, or the evidentiary value may be compromised.

THE HUMAN FACTOR: TRAINING, GOVERNANCE, AND COMMAND DECISION-MAKING

Running through this entire chapter is a thesis that can now be stated explicitly: the effectiveness of drones in security is not primarily a function of the equipment, but of the human and institutional competence that operates and governs it. This proposition turns conventional wisdom—which equates capability with hardware acquisition—on its head and shifts the focus to training, risk governance, and the quality of decision-making.

THE GAP BETWEEN KNOWING HOW TO FLY AND KNOWING HOW TO DECIDE

The most important distinction in training is the one that separates the technical skill of piloting from the decision-making competence of command. Knowing how to fly is necessary, but far from sufficient. An operator who has mastered the controls but does not understand risk analysis, the regulatory framework, the legal limits on image capture, and contingency procedures is a pilot, not an operations manager. By making prior authorization universal and operator responsibility sharper, the new regulatory architecture raises the importance of this decision-making competence: whoever commands the operation must master risk analysis, not just the technology. The experience in Pará offers an instructive model of institutionalized training, with classes of personnel from multiple agencies across the System trained through a systemic approach—not limited to handling the aircraft, but covering software, communications systems, ground control stations, and sensors; in other words, the RPAS as a whole.

EVALUATING TRAINING AND STRUCTURING RISK

Claiming that training is decisive means confronting an uncomfortable question: how do we know whether it worked? Simply issuing certificates says nothing about the competence actually acquired or whether it holds up over time. Rigorous evaluation distinguishes successive levels of evidence—participant reaction, demonstrated learning, behavior change in real operations, and institutional results, such as fewer incidents and shorter response times. Programs that measure only satisfaction or passing a written exam capture the most superficial and least predictive levels of effectiveness. For drone operators and managers, what matters is whether, months later, personnel correctly apply risk, contingency, and compliance procedures under the pressure of real operations. Risk governance, in turn, translates into a concrete cycle: identify risks—technical, legal,

privacy-related, airspace safety, and risks to people on the ground; assess them in terms of likelihood and severity; implement mitigations—contingency plans, emergency landing areas, link redundancy, altitude and proximity limits; and monitor continuously. The growing algorithmic autonomy of these platforms adds new risks—the reliability of automated detection, false positives and negatives, opaque decisions, and the need for meaningful human oversight—that governance must take into account. Established risk management frameworks organize this process into an iterative cycle of identification, assessment, mitigation, and monitoring (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2018), and dedicated frameworks for managing the risks of artificial intelligence systems extend this cycle to the risks introduced by algorithmic autonomy, emphasizing reliability, explainability, and meaningful human oversight (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2023). These frameworks become more relevant precisely to the extent that drones incorporate artificial intelligence: autonomous detection of people, navigation along predefined routes, and automated response to alarms shift part of the decision-making from the human operator to the system, requiring specific governance over the reliability and auditability of these processes. Governance, however, is not limited to the technical management of risk: it also encompasses the legal dimension—compliance with aviation regulations, data protection law, and constitutional guarantees—and the ethical dimension—proportionality, transparency, and accountability to society.

TRAINING AS AN ONGOING PROCESS

Effective training is an ongoing process, not a one-time event. The rapid technological evolution of the platforms, shifting threats, and the regulatory transition itself make knowledge perishable. Initial training, however robust, decays unless it is sustained by periodic refresher courses, hands-on exercises, and regulatory updates. Institutions that treat training as a one-off course that ends when the certificate is handed out condemn themselves to operating with outdated competence. The right approach is one of continuing education, in which training is renewed at the pace of the changes that make it necessary—a principle that

applies to field operators and, above all, to the managers who command operations.

An honest assessment must give equal weight to the technology's limitations. On the technical side, limited battery endurance restricts mission duration; adverse weather narrows the operational window; and dependence on the radio-frequency spectrum exposes operations to interference. On the cybersecurity side, the expanded attack surface calls for the precautions detailed in the section on the adversarial side. Finally, on the social side, public acceptance—a condition for institutional sustainability—depends on the ability to demonstrate proportionality and respect for rights; otherwise, a backlash driven by distrust may curtail legitimate and valuable uses (SABINO et al., 2022). There is also an equity dimension: vast, under-resourced territories, such as large swaths of the Amazon, tend to rely more heavily on unmanned aerial capability precisely where conventional resources are scarcest, which makes in-house training all the more decisive. The agenda for maturity is therefore less technological than institutional: it requires continuing education, robust governance, auditable compliance, and the patient building of public trust.

CASE STUDY: SIEDS AND GRAESP IN THE AMAZON BIOME

The experience of the State of Pará condenses the propositions of this chapter into a concrete case. The Public Security Air Group (GRAESP) was created by State Law No. 7,584 of December 28, 2011, which reorganized the State Public Security and Social Defense System (SIEDS), replacing the former Military Police air group and the Fire Department's air operations coordination office (PARÁ, 2011). Its mission is to plan, promote, and oversee the state's public security and civil defense air operations, integrating and optimizing the System's air assets. GRAESP's very origin—the unification of previously scattered assets—embodies the principle of integration that guides the state's security policy.

The operational adoption of drones within SIEDS brings together the dimensions discussed in this chapter. Technologically, the platforms address the challenges of a biome of dense forest, long rivers, and archipelagos, where thermal cameras and beyond-visual-line-of-sight range turn hostile terrain into operable territory. On the regulatory

side, operations are subject to the same federal architecture—ANAC, DECEA, ANATEL—under the new ICA 100-40 (BRASIL, 2026). Organizationally, coordination between the air and river groups and the integration of the various agencies embody the thesis that effectiveness depends on the institutional ecosystem that receives the technology. And on the human side, successive training classes, with a systemic approach and substantial course hours, show an understanding that competence is built through continuing education, not merely by acquiring equipment. The breadth of missions—from combating deforestation and illegal mining to search and rescue in archipelagos, from river monitoring to protecting the prison system against hostile drones, from supporting major events to integrated patrols—confirms that the drone, embedded in an architecture of governance and training, functions as a cross-cutting security tool. The lesson of this case extends beyond the state's borders: the equipment is the most easily replicated part; what distinguishes a mature operation is the institutional competence that employs it safely, compliantly, and legitimately.

The institutional maturity of the Pará case is also evident in its cross-sector reach and in its place within an ongoing modernization effort. Training was not confined to the air group: the corrections administration trained operators to counter hostile drone overflights of prison facilities, a front that combines, in a single problem, defensive use and the forensic examination of seized aircraft. The integration of the civil, military, and forensic police, the fire department, the corrections administration, and the air and river groups, under the coordination of the System, embodies the principle that technology delivers more when it is shared than when it is siloed within individual institutions. And ongoing investment in technology, vehicles, and bases—which in recent fiscal years has reached the System's agencies, including the air group—places drone adoption within a broader movement in which the equipment is merely the visible face of a transformation that depends, in order to bear fruit, on well-trained people and robust governance.

FINAL REMARKS

This chapter has examined the use of remotely piloted aircraft in public and private

security across three dimensions—technological, regulatory, and human—and has argued, throughout, a single unifying thesis: the effectiveness of these operations is not decided by the equipment, but by the architecture of competence, governance, and compliance that surrounds it. The platforms offer extraordinary capabilities for sensing, range, and early information, but these capabilities translate into real security only when they are operated by competent professionals, governed by robust risk frameworks, and subject to the legal and ethical limits that legitimize their use. Recent literature reinforces each of these points: the risk-based paradigm for operational deployment (CHEN et al., 2023), the centrality of public acceptance and trust (SABINO et al., 2022), the dependence of regulatory compliance on perceived legitimacy (HENDERSON; SHELLEY, 2023), and the need for forensic and defensive competence in the face of the technology's adversarial side (AL-DHAQM et al., 2021; CHAMOLA et al., 2021).

By consolidating and universalizing airspace access requirements as of July 2026, the new ICA 100-40 (BRASIL, 2026) closes the era of tolerated improvisation and opens the era of auditable compliance. For SIEDS managers—and for those of any security institution, public or private—this means that the competence required goes beyond flying skills: it is about mastering risk analysis, the regulatory framework, privacy limits, and command decision-making under uncertainty. The gap between knowing how to fly and knowing how to decide is, ultimately, the space that separates owning a piece of equipment from having a real capacity to produce security. For managers on the ground, the practical message is straightforward: invest in people and governance with the same commitment you put into equipment; build compliance before you fly; make continuing education a routine, not an event; incorporate risk analysis into command decisions; and, through transparency, earn the trust of the society you are sworn to protect. It is in this balance—between operational effectiveness and the protection of rights, between innovation and accountability—and not in the sophistication of the equipment, that the true measure of a successful security operation lies.

REFERÊNCIAS

AL-DHAQM, A.; IKUESAN, R. A.; KEBANDE, V. R.; RAZAK, S.; GHABBAN, F. M. Research challenges and opportunities in drone forensics models. Electronics, v. 10, n. 13, p. 1519, 2021.

BRASIL. Agência Nacional de Aviação Civil (ANAC). Regulamento Brasileiro da Aviação Civil Especial RBAC-E nº 94: requisitos gerais para aeronaves não tripuladas de uso civil [Special Brazilian Civil Aviation Regulation RBAC-E No. 94: general requirements for civil unmanned aircraft]. Brasília: ANAC, 2017. Updated in 2023.

BRASIL. Agência Nacional de Aviação Civil (ANAC). Consulta Pública nº 09/2025: proposta de RBAC nº 100 (Inovação nos Céus) [Public Consultation No. 09/2025: proposed RBAC No. 100 (Innovation in the Skies)]. Brasília: ANAC, 2025.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo (DECEA). ICA 100-40: aeronaves não tripuladas e o acesso ao espaço aéreo brasileiro [Unmanned aircraft and access to Brazilian airspace]. Approved by Portaria DECEA nº 2094/DNOR8, March 18, 2026. Rio de Janeiro: DECEA, 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD) [General Personal Data Protection Law]. Diário Oficial da União: Brasília, DF, 2018.

CHAMOLA, V.; KOTESH, P.; AGARWAL, A.; NAREN; GUPTA, N.; GUIZANI, M. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad Hoc Networks, v. 111, p. 102324, 2021.

CHEN, H.; GAO, X.; LI, H.; YANG, Z. A framework for the optimal deployment of police drones based on street-level crime risk. Applied Geography, v. 162, p. 103178, 2023.

DE BRUYN, C.; RALEBITSO-SENIOR, K.; SCOTT, K. R.; PANTER, H.; BEZOMBES, F. Search, detect, recover: a systematic review of UAV-based remote sensing approaches for the location of human remains and clandestine graves. Drones, v. 9, n. 10, p. 674, 2025.

DEL-REAL, C.; DÍAZ-FERNÁNDEZ, A. M. Lifeguards in the sky: examining the public acceptance of beach-rescue drones. Technology in Society, v. 64, p. 101502, 2021.

HENDERSON, I. L.; SHELLEY, A. Examining unmanned aircraft user compliance with Civil Aviation Rules: the case of New Zealand. Transport Policy, v. 133, p. 176-185, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31000: risk management — guidelines. 2nd ed. Geneva: ISO, 2018.

KOOTALA, A.; MOUSA, A.; PONG, P. W. Drones are endangering energy critical infrastructure, and how we can deal with this. Energies, v. 16, n. 14, p. 5521, 2023.

KUMAR, R.; AGRAWAL, A. K. Drone GPS data analysis for flight path reconstruction: a study on DJI, Parrot & Yuneec make drones. Forensic Science International: Digital Investigation, v. 38, p. 301182, 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: NIST, 2023. (NIST AI 100-1).

PAPYAN, N.; KULHANDJIAN, M.; KULHANDJIAN, H. et al. AI-based drone assisted human rescue in disaster environments: challenges and opportunities. Pattern Recognition and Image Analysis, v. 34, p. 169-186, 2024.

PARÁ (Estado). Lei nº 7.584, de 28 de dezembro de 2011. Reorganiza o Sistema Estadual de Segurança Pública e Defesa Social e cria o Grupamento Aéreo de Segurança Pública (GRAESP) [Reorganizes the State Public Security and Social Defense System and creates the Public Security Air Group]. Diário Oficial do Estado do Pará: Belém, PA, 2011.

SABINO, H.; ALMEIDA, R. V. S.; MORAES, L. B. de; SILVA, W. P. da; GUERRA, R.; MALCHER, C.; PASSOS, D.; PASSOS, F. G. O. A systematic literature review on the main factors for public acceptance of drones. Technology in Society, v. 71, p. 102097, 2022.

SALAMH, F. E.; KARABIYIK, U.; ROGERS, M. K.; MATSON, E. T. A comparative UAV forensic analysis: static and live digital evidence traceability challenges. Drones, v. 5, n. 2, p. 42, 2021.

YEOM, S. Thermal image tracking for search and rescue missions with a drone. Drones, v. 8, n. 2, p. 53, 2024.