

Governing low-altitude security: a comparative analysis of the safety–security nexus in unmanned aircraft governance across the United States, the European Union and Singapore

Wenhao Gao

gaowenhao@ppsuc.edu.cn

People's Public Security University of China

Article

Keywords:

Posted Date: October 13th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10990742/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Unmanned aircraft compress two distinct dimensions of security—operational safety and national and public security—into a single flying object that cannot easily be disaggregated before flight. As the low-altitude economy expands, this compression has turned airspace below one kilometre into a domain where accidental and hostile risks are tightly coupled, yet comparative research on how states institutionally integrate these two dimensions remains scarce. Addressing this gap, the study asks how leading jurisdictions govern the safety–security nexus in unmanned aircraft, and why they arrive at divergent institutional configurations. Drawing on securitisation theory and risk-governance scholarship, it develops an institution–technology–ideation framework and applies it through a qualitative comparative analysis of policy and regulatory documents from the United States, the European Union and Singapore. The analysis yields a governance typology of three configurations: securitisation-driven but fragmented authority (United States); an integrated market coupled with fragmented defence (European Union); and integrated, precise regulation enabled by a city-state scale (Singapore). Where each jurisdiction lands is explained by the interaction of two variables: the degree of constitutional and administrative concentration, and the intensity of threat perception. The comparison shows that risk-based tiered authorisation and digitally enabled airspace awareness have become common practice, whereas the capacity to integrate the two faces of security institutionally is decisive. The article situates China within this typology and argues that integrating safety and security—rather than expanding protective measures alone—is the central governance challenge for emerging low-altitude airspace.

Introduction

The airspace immediately above cities is being opened for economic use at unprecedented speed. Framed in China and elsewhere as a “low-altitude economy,” unmanned aircraft are entering logistics, inspection, agriculture, emergency response and passenger transport, and are widely promoted as an engine of new productive capacity. Yet the same devices that carry commercial promise also carry risk: they are cheap, easy to operate and difficult to detect, and a photography drone can be modified within minutes to carry contraband or explosives. The governance question raised by this diffusion is therefore not merely how to make flight safe, but how to organise, institutionally, the protection of a shared and increasingly crowded airspace against both accidental and deliberate harm.

This question is sharpened by a linguistic and conceptual feature that the English literature captures through the distinction between *safety* and *security*. Safety concerns protection against accidents and technical failure; it is operational and largely the province of civil-aviation authorities. Security concerns protection against hostile and intentional acts; it is political and typically the province of policing, homeland-security or defence agencies. In most domains these two dimensions can be institutionally separated, each with its own agencies, legal bases and expert communities. Unmanned aircraft are distinctive because they compress both dimensions into a single object and a single flight, and because the line between benign and hostile use often cannot be drawn *ex ante*. This is the tension this article calls the safety–security nexus, and low altitude is where it is most acute.

Existing scholarship has approached low-altitude governance largely through three lenses: the design of regulatory and legal frameworks (Pagallo and Bassi 2020); the assessment of operational and collision risk (Clothier et al. 2015; Horowitz et al. 2016); and, more recently, the social and political dimensions of drone deployment, including privacy and surveillance (Lee et al. 2022). These strands have advanced understanding of what should be regulated and of the risks involved. They have paid less attention, however, to a prior and more structural question: given that safety and security are institutionally organised in different ways across states, how do those governance arrangements shape a jurisdiction's capacity to manage unmanned aircraft as a dual object of safety and security? The variation lies less in the protective measures adopted than in the institutional configurations through which they are regulated, coordinated and implemented.

This article addresses that gap. It asks two connected questions. First, how do leading jurisdictions institutionally govern the safety–security nexus in unmanned aircraft? Second, why do they arrive at divergent configurations? To answer them, the study develops an institution–technology–ideation framework grounded in securitisation theory and risk-governance scholarship, and applies it through a qualitative comparative analysis of the United States, the European Union and Singapore—three jurisdictions selected to maximise institutional variation. It then situates China within the resulting typology, treating it as an analytically instructive case rather than as the object of the analysis.

The article makes three contributions. Conceptually, it reframes low-altitude governance around the institutional integration of safety and security, rather than around the accumulation of individual protective technologies. Analytically, it proposes a typology of three governance configurations and offers a two-variable explanation—constitutional concentration and threat perception—for why jurisdictions occupy different positions within it. Empirically, it provides a structured comparison of three contrasting cases and locates China within the same analytical space, generating propositions that travel beyond any single national context.

The safety–security nexus: an analytical framework

Unmanned aircraft as a dual object of safety and security

The starting point of the analysis is that unmanned aircraft cannot be assigned cleanly to either the safety or the security domain. Three properties account for this. First, in physical terms, small consumer and industrial drones are low, slow and small; often built from non-metallic materials, they present a minimal radar cross-section and hug terrain, rendering them nearly invisible to conventional air-defence detection. Second, in terms of accessibility, their low cost and ease of operation mean that almost any individual can put an aircraft aloft within minutes, so the governed population expands from a bounded set of aviation enterprises to a vast and dispersed body of operators. Third, in functional terms, a single airframe can serve inspection or delivery one day and, after minor modification, carry prohibited items the next; the distance between benign and hostile use is thin.

The Collingridge dilemma is visible here: while a technology is still malleable its risks are poorly understood, and by the time those risks are manifest the technology is already deeply embedded and difficult to reshape (Collingridge 1980). The stronger the industrial drive to diffuse low-altitude flight, the narrower the window left for institutional response. This compression is especially severe at low altitude because the airspace within a kilometre of the ground is simultaneously the most densely populated space of urban life and a blind spot for both air-defence and air-traffic systems: too low for national air-defence radar, yet too close to airports, critical sites and crowds. Where dense civilian flight and sensitive security targets overlap in the same near-ground layer, accidental and hostile risks are bound together as never before.

Three tensions

Treating unmanned aircraft as a dual object implies that low-altitude governance must manage three interlocking tensions, any neglect of which propagates into systemic imbalance.

The first is the tension between development and security. The low-altitude economy is promoted as a driver of new productive capacity, which favours open airspace and light-touch approval; security, by contrast, requires that flight be controllable, traceable and, if necessary, interruptible. The two are not zero-sum, but they are continually renegotiated in the calibration of specific rules: too permissive, and unauthorised flight proliferates; too restrictive, and innovation is stifled.

The second is the tension between openness and control, the spatial projection of the first. Effective governance does not prohibit flight wholesale but distinguishes, spatially, between zones that may be opened and zones that must be controlled. The European Union's open, specific and certified categories, Singapore's permit-based zoning, and China's division of airspace into controlled and suitable-for-flight zones are variations on this same logic, and each must be adjusted dynamically to time, event and evolving risk.

The third is the tension between integration and fragmentation, the dimension most easily overlooked but most consequential institutionally. Because security spans operational and defensive meanings and implicates air-traffic, civil-aviation, policing, industry and even military actors, governance confronts a basic choice: to integrate dispersed competences into a coherent system, or to leave them distributed across agencies that act separately. Securitisation theory is instructive here: when an issue is constructed as an existential threat and handed to security actors for extraordinary treatment, it is lifted out of ordinary politics (Buzan et al. 1998). The paradox of low altitude is that it must be securitised enough to command defensive resources and counter-drone authority, yet desecuritised enough to accommodate large-scale everyday economic use. Risk-governance scholarship reinforces the point: modern technologies systematically manufacture risk, and the task of governance is not to eliminate risk—which is neither possible nor compatible with development—but to hold it within socially tolerable thresholds through institutional means (Beck 1992). Governing the nexus thus requires a dynamic balance of securitisation and desecuritisation rather than either alone.

The institution–technology–ideation framework

On this basis, the article analyses each jurisdiction along three dimensions. The institutional dimension concerns the regulatory basis and the distribution of authority: the mode of legislation (a dedicated statute or provisions grafted onto existing aviation law), the allocation of competences (concentrated or dispersed), and the mechanisms of coordination across levels of government and between civil and military actors. The technological dimension concerns three enabling capabilities: the digital management of airspace (for example unmanned-aircraft traffic management, the European U-space, or an integrated national supervisory platform); the remote identification of aircraft; and the detection of, and response to, non-cooperative targets. The ideational dimension concerns the ordering of values: whether development or security takes priority, the degree to which operational and public safety are integrated, and how the openness–control tension is resolved.

Positioning the cases on two axes—the degree of securitisation (whether governance is driven by a security or a developmental logic) and the structure of authority (integrated or fragmented)—yields a typological map of governance models (Fig. 1). Crucially, where a jurisdiction lands is not accidental. It can be explained by the interaction of two variables: the degree of constitutional and administrative concentration, which determines whether security competences can be integrated and directed; and the intensity and character of threat perception, which determines how far governance is driven by a security logic. The former is a structural variable, the latter a perceptual one, and their interaction shapes a jurisdiction's position on both axes. This two-variable account forms the causal spine of the comparison and provides the coordinates against which the Chinese case is later assessed.

Data and methods

The study employs a qualitative comparative design. Its purpose is to identify recurring governance configurations across contrasting institutional settings rather than to achieve statistical representativeness. Three jurisdictions—the United States, the European Union and Singapore—were selected through purposive sampling according to two criteria. First, each has developed a comparatively articulated national or supranational framework for governing unmanned-aircraft safety and security, making it analytically substantive. Second, together they span markedly different administrative traditions and degrees of centralisation—a federal system, a supranational union of sovereign states, and a unitary city-state—providing the institutional contrast on which comparative analysis depends. China is examined separately, after the typology has been established, as an instructive additional case rather than as a fourth comparator.

The empirical corpus consists of publicly available policy and regulatory documents in force at the time of analysis. It comprises primary legislation, executive orders, implementing regulations, technical standards and official guidance issued by national or supranational authorities with regulatory competence over civil aviation, airspace, internal security or defence—for example, in the United States, Executive Orders 14305 and 14307 and the Federal Aviation Administration's proposed Part 108; in the

European Union, Implementing Regulations (EU) 2019/947 and 2019/945 and the U-space regulations; and in Singapore, the Unmanned Aircraft (Public Safety and Security) Act 2015 and the Air Navigation (Unmanned Aircraft Operations) Regulations. Documents issued solely at the sub-national or municipal level, together with media reports, advocacy materials and secondary scholarship, were excluded from the analytical corpus; the latter were consulted only to contextualise and interpret the primary material.

The documents were analysed through systematic qualitative content analysis combining deductive and inductive coding. In the first stage, material was coded deductively against the three analytical dimensions of the framework—institution, technology and ideation—and their sub-components. In the second stage, additional governance elements emerging from the documents were identified inductively. Where feasible, instruments were examined in their original language and cross-checked against official English translations to ensure terminological consistency. The governance typology reported below was derived inductively from this comparative reading rather than imposed a priori; it should therefore be read as a set of analytical configurations describing recurring institutional arrangements, not as a normative ranking. Because the analysis relies on documentary evidence, it captures the institutional design of low-altitude governance rather than its implementation or measured effectiveness—a limitation revisited below.

Comparative analysis

The United States: securitisation-driven, fragmented authority

The United States exhibits ambition and anxiety in equal measure. On 6 June 2025 the administration signed two executive orders on the same day that display this dual disposition. Executive Order 14307, “Unleashing American Drone Dominance,” foregrounds development, commercialisation and export, directing the Federal Aviation Administration (FAA) to normalise beyond-visual-line-of-sight (BVLOS) operations, expand test ranges and establish integrated pilot programmes for electric vertical take-off and landing (eVTOL) aircraft, and instructing the Department of Defense to expand a “blue list” of domestically produced, compliant airframes so as to reduce dependence on foreign-manufactured drones (Exec. Order No. 14307 2025). Executive Order 14305, “Restoring American Airspace Sovereignty,” opens in a near-alarmist register, warning that criminals, terrorists and hostile foreign actors are intensifying the weaponisation of drones and that critical infrastructure faces repeated unidentified incursions (Exec. Order No. 14305 2025). It establishes a federal task force, directs the FAA to accelerate restrictions on flight over critical infrastructure, and instructs the Departments of Justice and Homeland Security to open funding channels for detection equipment to state, local, tribal and territorial (SLTT) law-enforcement agencies.

On the industrial side, securitisation quickly translated into action. On 7 August 2025 the FAA released its proposed Part 108, a rule of more than seven hundred pages that would replace nearly a decade of case-by-case waivers with a performance- and risk-based framework (FAA 2025). The rule sorts operating

areas into five risk categories by population density, distinguishes permitted operations from operating certificates, shifts the locus of responsibility from individual pilots to operating organisations, mandates detect-and-avoid, remote identification and continuous position tracking, and introduces automated data-service providers to furnish traffic-management services. This risk-defines-the-rule logic parallels the European Union's Specific Operations Risk Assessment (EASA 2025; Pagallo and Bassi 2020). At the same time, the Federal Communications Commission moved in December 2025 to bar the distribution of new foreign-manufactured drones on national-security grounds, folding supply-chain security into the ambit of low-altitude governance (FCC 2025).

The governance reach of the United States is thus extending in two directions: upstream into the supply chain, welding industrial to national security through the blue list and import restrictions; and outward toward critical infrastructure, building on Section 2209 of the 2016 FAA Extension, Safety, and Security Act (2016), which authorised flight restrictions over sensitive facilities. Both directions strengthen control, sitting in tension with Part 108's loosening of operational access—the American expression of the safety–security nexus's internal contradiction.

Yet the deepest fault line is not insufficient ambition but fragmented authority. Constrained by federalism and existing law, statutory authority to counter drones—to jam, force down or destroy them—has long been confined to a few federal agencies, while state and local police and the operators of critical infrastructure, though on the front line of the threat, generally lack even the authority to detect (Feddersen 2025). The public alarm and official confusion generated by a series of unidentified drone sightings over New Jersey in late 2024 illustrate this predicament. Executive Order 14305 deliberately separates detection from response—liberalising the former, restricting the latter—reflecting how, under traditions of civil liberty and constrained federal power, securitising discourse can mobilise attention yet struggle to breach institutional silos.

The federal counter-drone authority is itself unstable. The statutory basis for the Departments of Homeland Security and Justice, the Preventing Emerging Threats Act of 2018 (codified at 6 U.S.C. § 124n), was designed from the outset as a four-year measure; it lapsed in October 2022 and was thereafter sustained by successive short-term extensions (Preventing Emerging Threats Act 2018). That even core federal competence required repeated renewal exposes how difficult institutional integration is under a tradition of separated powers. Relief came only late in 2025: the National Defense Authorization Act for Fiscal Year 2026, signed on 18 December 2025, amended § 124n to authorise, for the first time, trained and certified SLTT agencies to conduct counter-drone operations, extending the authority to September 2031 (National Defense Authorization Act 2026). This remains a conditional, incremental patch: implementing regulations and equipment lists are still to be issued, and full certification will take time. The United States required seven years, and the vehicle of a defence-authorisation act, to open even a narrow path for local response—securitising discourse leading, institutional integration lagging.

The European Union: an integrated market, fragmented defence

If the American weakness runs vertically between federal and local levels, the European Union's runs horizontally between market and defence, and it is exposed with greater drama. On the operational-safety side, the Union is a model of transnational integration. Built on Implementing Regulations (EU) 2019/947 and 2019/945, together with the 2021 U-space regulations, it has established a single rulebook spanning twenty-seven member states and associated countries (Regulation (EU) 2019/947, 2019). Its core is a risk-based tripartite scheme: the low-risk open category requires no prior authorisation; the medium-risk specific category requires risk assessment and authorisation; and the high-risk certified category is treated akin to manned aviation. To standardise the specific category, the Union adopted the Specific Operations Risk Assessment (SORA), updated to version 2.5 in September 2025 to accommodate autonomy and AI-assisted operations (EASA 2025). A single SORA authorisation grants access to more than thirty national markets—an assess-once, apply-everywhere dividend no single national rulebook can match (Pagallo and Bassi 2020).

Alongside rule integration, the Union has pursued the digital management of airspace. The U-space framework envisages network identification, geo-awareness, flight authorisation and dynamic-restriction services delivered by certified providers. Yet paper design and delivery capacity diverge: in most member states U-space airspace remains at the designation and pilot stage, and large-scale operation has yet to arrive. More intractable is the gap between detection and response. Radio-frequency detection often fails against silent, pre-programmed autonomous drones, and physical counter-measures over densely populated European airspace are constrained by both collateral-damage and legal-authority considerations. A threat that can be sensed cannot necessarily be intercepted—a limitation soon exposed in a wave of airport crises.

The autumn of 2025 revealed the fragility of this sophisticated system. On the night of 22 September, several large drones repeatedly entered controlled airspace at Copenhagen Airport, forcing the closure of Denmark's busiest hub for nearly four hours and disrupting scores of flights, with Oslo also briefly closing its airspace (The New York Times 2025). Aalborg and Billund followed in the ensuing days; on 2–3 October, Munich Airport twice suspended operations within twenty-four hours, stranding more than three thousand passengers overnight. Danish authorities characterised the incidents as a hybrid operation conducted by a professional actor. Drone incidents near European critical infrastructure reportedly tripled between 2024 and 2025; in the same period some twenty Russian drones entered Polish airspace, prompting NATO to scramble aircraft at a cost exceeding one million euros per sortie. Cheap and hard-to-trace drones have become an asymmetrically costly instrument of hybrid conflict (Horowitz et al. 2016).

The root of the problem is the Union's horizontal division. Operational safety is highly communitised, whereas defence and security remain firmly in member-state hands, each with its own priorities and budgets. On 16 October 2025 the European Commission proposed a European Drone Defence Initiative within its Defence Readiness Roadmap 2030, seeking a multi-layered, interoperable detection-tracking-defence system (DRONELIFE 2025). Turning the initiative into capability, however, must cross fragmented procurement, divergent standards, and civil–military and EU–NATO coordination. In short,

the Union has achieved a single market in operational safety but is trapped in fragmented defence, and the seam between them is precisely where hybrid threats repeatedly penetrate. Tellingly, the legal mandate of the European Union Aviation Safety Agency is confined to safety; security and defence lie beyond its remit—the institutional boundary between civil safety regulation and national-security defence proving the hardest to suture.

Singapore: integration and precision at a city-state scale

Against the expansive, layered systems of the United States and the European Union, the city-state of Singapore offers another possibility: precision achieved through smallness of scale. As early as 2015 Singapore enacted the Unmanned Aircraft (Public Safety and Security) Act, whose very title expresses its governing philosophy: by placing public safety and security within a single statute, it refuses their separation at the legislative source (Unmanned Aircraft Act 2015). This integration, built into the institutional genome, is precisely what the American and European models lack.

On this basis the Civil Aviation Authority of Singapore (CAAS), as the lead agency, has constructed a graduated yet clearly bounded regime under the Air Navigation (Unmanned Aircraft Operations) Regulations. All drones above 250 grams must be registered; the altitude ceiling is compressed to about sixty metres, half the internationally common 120-metre standard, among the strictest in the world—a necessary price of safety and order in a land-scarce state whose Changi airspace is intensely busy (CAAS 2024). Commercial and non-recreational operations require both an operator permit and an activity permit, pilots must hold a licence, and the official OneMap/FlyWhere platform overlays no-fly, restricted and temporary-restricted zones on a real-time map.

Most notable is an arrangement that is integrated yet coordinated. Although CAAS is the single lead agency, security-sensitive matters draw in other bodies: flights over sensitive sites require police clearance, and radio-frequency use must comply with the media-development authority's rules; during national events, temporary restricted zones are designated and unauthorised flight is criminalised. In enforcement, CAAS and the police deploy detection and counter-measures backed by heavy penalties. Singapore's experience is instructive but its transferability is constrained by scale: a compact territory, unitary airspace and concentrated administrative capacity make it feasible for one statute to integrate safety, one platform to manage airspace and one permit chain to run throughout. This heavily permit-dependent model is, however, relatively closed; its strict ceilings and broad permit requirements constrain operators seeking scale. Singapore trades a measure of openness for a high degree of control and integration—a choice rooted in its geography and security environment rather than a rank-orderable optimum.

A typology of low-altitude security governance

Read together within the institution–technology–ideation framework, the three cases fall into distinct configurations (Table 1). Viewed longitudinally, they share three convergent lessons. First, risk-based

tiered authorisation has become standard practice: the American five-tier scheme, the European open-specific-certified division with SORA, and Singapore's use- and weight-based permits all abandon blanket permission-or-prohibition in favour of matching regulatory intensity to operational risk (Baldwin and Black 2008). Second, digitally enabled airspace underpins governance: UTM, U-space and OneMap alike translate physical airspace into a data space that can be sensed, scheduled and traced, with remote identification serving as the technical precondition for area-wide awareness and enforcement. Third, the integration of the two faces of security is repeatedly confirmed as the crux of success: the American and European difficulties both stem from insufficient integration, whereas Singapore's strength lies precisely in achieving it. A further, quieter commonality is telling: all three respond through dedicated, higher-order legislation or executive action rather than by piecemeal amendment of existing aviation law, reflecting a shared recognition that low altitude is a new governance domain requiring purpose-built institutions.

Table 1

A typology of low-altitude security governance in the United States, the European Union and Singapore.

Dimension	United States	European Union	Singapore
Dominant logic (ideation)	Securitisation-driven; industrial ambition and security anxiety coexist	Integrated operational safety; nationalised security and defence	Public safety and security jointly prioritised; order first
Legislative mode (institution)	Executive orders plus federal rules; dedicated, incremental	Unified regulations plus member-state competence; two-tier	Single integrating statute (2015 Act)
Authority structure (institution)	Federal-led; vertical federal-local fragmentation	Communitised market; fragmented defence	Single lead agency plus multi-agency coordination
Risk tiering (technology)	Part 108: five tiers by population density	Open/specific/certified plus SORA	Tiered by use and weight; permit classes
Airspace digitalisation (technology)	UTM plus automated data services (Part 146)	U-space plus certified service providers	OneMap/FlyWhere plus real-name registration
Detection and counter-drone authority	Federal-led; SLTT authority long absent, recently opening	EDDI nascent; nationally dispersed	CAAS plus police coordination; strict enforcement
Degree of integration	Low: safety and defence separated; vertically split	Medium-low: market integrated, defence fragmented	High: integration achieved at the legislative source
Principal weakness	Safety-defence separation; slow civil-military and central-local coordination	Fragmented defence; hybrid threats penetrate	Scale-dependent; limited openness for industry

Source: compiled by the author from the regulatory and official documents cited above.

Viewed cross-sectionally, two unresolved problems stand out. The first is the pervasive ambiguity of detection and counter-drone authority. All three face a common bottleneck—detection is comparatively easy, response hard—because radio-frequency detection frequently fails against silent, autonomous flight while active counter-measures are constrained by interference and ground-safety risks; the American SLTT gap and the European national dispersion are both expressions of it. The second is the dynamic imbalance between development and security: the United States pushed industrial primacy through securitising discourse yet left local protection exposed; the European Union prized its single market yet underestimated the cost of fragmented defence; Singapore secured order through stringent control yet constrained industrial imagination. Low-altitude governance admits no once-and-for-all optimum; it is a balance that must be continually recalibrated.

Situating China within the typology

Placed within these coordinates, China constitutes an analytically instructive case. Its institutional backbone is the Interim Regulations on the Administration of Unmanned Aircraft Flight, in force since 1 January 2024—the country’s first dedicated administrative regulation for drones. Comprising sixty-three articles, it applies whole-chain management from design and production to operation, and establishes four basic systems: classified management, airspace designation, real-name registration and qualification management (Interim Regulations 2024). Aircraft are sorted into micro, light, small, medium and large classes; airspace is divided into controlled and suitable-for-flight zones, the former requiring approval and the latter opened to low-risk types; owners must register under their real names, aircraft must carry a unique product identifier, and larger types and their operators require airworthiness approval and licences.

Distinctive in comparative terms is the regulation’s allocation of authority. A national air-traffic-management leading body directs unmanned-aircraft flight management nationwide, with civil-aviation, public-security, industry and market-supervision authorities responsible according to their remits and local governments exercising territorial management. This civil–military integration and cross-departmental coordination allows unified scheduling of civil and military airspace, forestalling at the institutional source the vertical federal–local split observed in the United States. In parallel, an integrated national supervisory platform (UOM) performs registration, airworthiness, air-traffic and operational functions (Ministry of Transport 2024). The framework continues to be reinforced: from 1 May 2026, mandatory national standards require aircraft to report identity, position, speed and status to regulators in real time throughout flight, marking a shift from ex post accountability to continuous real-time supervision.

Against the international backdrop, three comparative strengths are discernible. The first is ideational integration. Where the American and European difficulties trace to the separation of operational and defensive security, China places aviation, public and national security together as a continuous spectrum in the legislative purpose, refusing their division at the conceptual source; this does not abolish the division of labour but provides dispersed agencies with a shared value coordinate. The second is the combination of civil–military integration and platform capacity, which affords regulators comparatively

strong area-wide awareness and traceability. The third is that industrial position can be converted into a governance instrument: China's leading role in the civil-drone supply chain makes it possible to embed safety requirements in product design and standards, achieving compliance-by-manufacture in a way that import-dependent economies cannot easily match.

Yet, held up to the same comparative mirror, China faces several challenges. Coordinated supervision is legislated but the boundaries of competence, information-sharing and joint response among civil-aviation, public-security, industry, market-supervision and military actors remain to be specified; how the safety interface (operational) meets the security interface (public and national) will determine whether the nexus is genuinely integrated or re-fragmented at departmental seams. Detection and counter-drone authority present a normative gap: which actors may, under what circumstances, by what procedure, and with what intensity detect and respond—particularly the authority of local police and infrastructure operators—remains under-specified, a Chinese version of the American SLTT problem. Risk tiering could be more fine-grained: current classification rests on static physical indicators such as weight and dimension, and lacks a scenario-based instrument comparable to SORA for dynamically assessing operational risk, leaving urban, beyond-visual-line-of-sight and swarm operations, and eVTOL inter-city transport, under-served by rule. Finally, real-time reporting throughout flight, while greatly enhancing control, entails the continuous aggregation of sensitive trajectory and imagery data, raising a data-security and privacy tension that a regime of continuous supervision must confront.

Discussion

The comparison supports a claim that is the article's principal contribution: the decisive variable in low-altitude security governance is not the protective technologies a jurisdiction deploys but whether it can institutionally integrate the two faces of security. Across the three cases, similar categories of measure—risk-based authorisation, digital airspace, remote identification, detection and counter-measures—recur; the principal variation lies in the governance arrangements through which those measures are regulated, coordinated and integrated. This is consistent with risk-governance scholarship holding that public institutions respond to uncertain threats not only by adopting new measures but by developing arrangements that structure responsibility, accountability and coordination.

The two-variable account developed above explains the observed positions. High threat perception combined with a fragmented constitutional structure yields the American pattern of ample securitisation but weak integration; a communitised market alongside nationalised defence yields the European pattern of an integrated market and fragmented defence; a highly concentrated city-state structure in a sensitive security environment yields Singapore's integrated model; and an ideationally integrating doctrine yields China's conceptual integration, whose challenge is to convert that ideational advantage into structural and mechanical coordination. No single model is universally applicable: jurisdictions pursue similar objectives through markedly different institutional pathways, and governance capacity emerges from the interaction of regulatory clarity, organisational coordination and institutional competence rather than from the accumulation of measures alone.

These findings carry implications for policy learning. Because comparable objectives are reached through divergent arrangements, policy transfer should focus less on replicating individual measures than on understanding the institutional conditions under which they operate. For jurisdictions confronting the safety–security nexus, three propositions follow: overlay scenario-based authorisation on static classification to refine risk tiering; clarify the allocation and standards of detection and counter-drone authority, distinguishing detection from active response; and enhance the public accessibility of digital airspace platforms so that lawful flight is easier than unlawful flight. For China specifically, the analysis suggests that the route forward lies not in importing any single foreign model but in converting ideational integration into coordinated mechanisms across central and local, civil and military, and public and private actors, while balancing continuous supervision against data protection.

Limitations and future research

Three limitations qualify these findings. First, the analysis rests on national and supranational policy and regulatory documents; it therefore examines the institutional design of low-altitude governance rather than its implementation or measured effectiveness, and gaps may exist between formally established arrangements and everyday practice. Second, the comparison focuses on three cases selected to maximise institutional variation rather than statistical representativeness; the proposed typology should be read as a set of analytical configurations derived from these cases rather than an exhaustive classification, and future work incorporating additional jurisdictions could refine, validate or extend it. Third, the study concentrates on the governance of physical safety and security against operational and intentional risks; other dimensions of low-altitude governance—notably privacy, data protection and the environmental effects of dense drone operations—are addressed only where they bear directly on the safety–security nexus. Future research could complement this institutional analysis with implementation studies, incident-based process tracing, or quantitative measurement of the association between governance configurations and safety-security outcomes.

Conclusion

The low altitude opened by unmanned aircraft is a mirror of the relationship between development and security. In a space that carries both enormous industrial promise and multiple security risks, operational safety and national security are compressed into a single flying object, forcing governors to confront an old question in new form: how to hold a line while preserving vitality. The United States pressed industrial primacy through securitising discourse yet was hampered by fragmented federal–local authority; the European Union achieved an integrated market in operational safety yet was penetrated at the seam of fragmented defence; Singapore attained integrated, precise governance through the advantages of a city-state yet paid in constrained openness. The three models are projections of the same safety–security tension onto different institutional soils. China, guided by an integrating doctrine and centred on a dedicated whole-chain framework, holds comparative advantages in ideational integration, civil–military coordination and platform capacity, yet must still recalibrate departmental coordination, counter-drone authority, risk tiering and data protection. The wider lesson is that low-altitude security governance

is never a once-and-for-all design but a continual balancing of development and security, and that the capacity to integrate the two faces of security—institutionally, not merely technologically—is what distinguishes governance that works from governance that does not. As international rule-making in this domain remains unsettled, the question of how to integrate safety and security within a single governance framework is one that no jurisdiction can escape.

Declarations

Data availability

All data analysed in this study are publicly available policy and regulatory documents. The full list of the legislative, regulatory and official documents that constitute the analytical corpus, together with the coding framework, is provided in the Supplementary Information. No new datasets were generated during the current study.

Competing interests

The author declares no competing interests, financial or non-financial. The author holds no relevant financial holdings, patents, consultancies or paid advisory roles, and has no business or family interests that could be perceived to influence the work reported in this article.

Ethics approval

This article did not involve human participants, their data or biological material, or any live subjects. Ethics approval was therefore not required.

Informed consent

This study did not involve human participants; informed consent was therefore not applicable.

Author contributions

Wenhao Gao is the sole author and is solely responsible for the conceptualisation, design, analysis, drafting and revision of the manuscript.

Funding

This work was supported by a Major Project of the National Social Science Fund of China (grant number 25&ZD267).

References

1. Baldwin R, Black J (2008) Really responsive regulation. *Mod Law Rev* 71(1):59–94.
2. Beck U (1992) *Risk society: towards a new modernity*. Sage, London.

3. Buzan B, Wæver O, de Wilde J (1998) *Security: a new framework for analysis*. Lynne Rienner, Boulder.
4. Civil Aviation Authority of Singapore (CAAS) (2024) Unmanned aircraft. Available at: <https://www.caas.gov.sg/> (accessed 2026).
5. Clothier RA, Greer DA, Greer DG, Mehta AM (2015) Risk perception and the public acceptance of drones. *Risk Anal* 35(6):1167–1183.
6. Collingridge D (1980) *The social control of technology*. St. Martin's Press, New York.
7. DRONELIFE (2025) European Drone Defence Initiative. 17 October. Available at: <https://dronelife.com/> (accessed 2026).
8. EASA (European Union Aviation Safety Agency) (2025) Specific operations risk assessment (SORA), version 2.5. EASA, Cologne.
9. Exec. Order No. 14305 (2025) Restoring American Airspace Sovereignty. 90 Fed. Reg. (6 June).
10. Exec. Order No. 14307 (2025) Unleashing American Drone Dominance. 90 Fed. Reg. (6 June).
11. FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, §2209 (2016).
12. Federal Aviation Administration (FAA) (2025) Normalizing unmanned aircraft systems beyond visual line of sight operations. Notice of Proposed Rulemaking, 7 August.
13. Federal Communications Commission (FCC) (2025) FCC bars authorisation of new unmanned aircraft systems from entities on the Covered List. Report and Order, FCC DA- 25-1086, 22 December. FCC, Washington, DC.
14. Feddersen B (2025) Restoring American airspace sovereignty. Commentary. Available at: <https://www.newamerica.org/> (accessed 2026).
15. Horowitz MC, Kreps SE, Fuhrmann M (2016) Separating fact from fiction in the debate over drone proliferation. *Int Secur* 41(2):7–42.
16. Interim Regulations on the Administration of Unmanned Aircraft Flight (2024) State Council and Central Military Commission Order No. 761, effective 1 January 2024.
17. Lee D, Hess DJ, Heldeweg MA (2022) Safety and privacy regulations for unmanned aerial vehicles: a multiple comparative analysis. *Technol Soc* 71:102079.
18. Ministry of Transport of China (2024) Rules for the operational safety management of civil unmanned aircraft (CCAR-92), effective 1 January 2024.
19. National Defense Authorization Act for Fiscal Year 2026, Pub. L. (18 December 2025), amending 6 U.S.C. §124n.
20. Pagallo U, Bassi E (2020) The governance of unmanned aircraft systems (UAS): aviation law, human rights, and the free movement of data in the EU. *Minds Mach* 30:439–455.
21. Preventing Emerging Threats Act of 2018, Division H of Pub. L. No. 115-254, codified at 6 U.S.C. §124n (2018).
22. Regulation (EU) 2019/947 (2019) On the rules and procedures for the operation of unmanned aircraft (with Regulation (EU) 2019/945 and Regulations (EU) 2021/664–666 on the U-space framework).

23. The New York Times (2025) Drone sightings force Copenhagen and Oslo airports to close temporarily. The New York Times, 22 September. Available at: <https://www.nytimes.com/2025/09/22/world/europe/copenhagen-oslo-airport-closed-drone.html> (accessed 2026)

24. Unmanned Aircraft (Public Safety and Security) Act 2015 (Singapore).

Figures

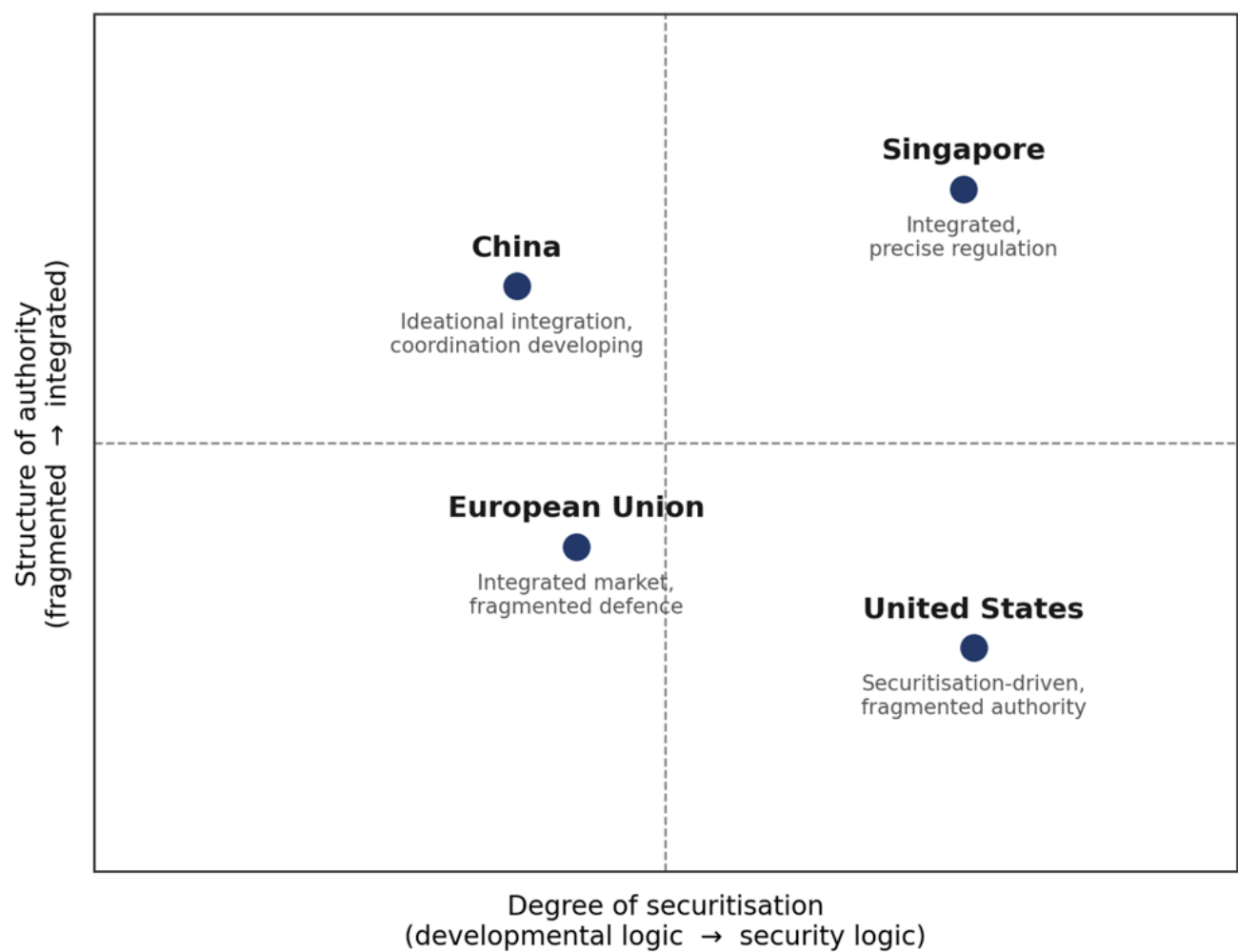


Figure 1

A typological map of low-altitude security governance. The horizontal axis represents the degree of securitisation (governance driven by a developmental logic on the left, by a security logic on the right); the vertical axis represents the structure of authority (fragmented below, integrated above). The United States occupies the securitisation-driven, fragmented quadrant; the European Union occupies an integrated-market yet fragmented-defence position; Singapore approaches the integrated, precise-regulation ideal type; and China achieves ideational integration with practical coordination still developing. Source: prepared by the author.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [SupplementaryInformation.docx](#)