

The Terminal Residual:

Warning Time and the Structural Limits of Small-UAS Defense

Terminal defense against low, slow, small drones over populated areas is a structural gap common to states across regime types.

DOCUMENT	VERSION	DATE
WP-2026-D2	V1.6	2026-10-01
AUTHOR	ORGANIZATION	SERIES
COLLIN GEORGE	SANCTIR LLC	PAPER II OF THREE

UNCLASSIFIED // OPEN SOURCE · NOT OFFICIAL U.S. GOVERNMENT ANALYSIS

Paper record

SERIES	DRONE THREATS TO POLITICAL LEADERSHIP: CAPABILITY, DEFENSE, AND AUTHORITY
AUTHOR	Collin George, Founder, Sanctir LLC ¹
PAPER	Paper II of three — The Terminal Residual
DOCUMENT	WP-2026-D2 · v1.6 · 2026-10-01
SCOPE	Effectiveness and limits of counter-UAS defense against small drones threatening political leadership, compared across regime types.
SOURCES	Open source only. Bluebook (21st ed.) citations; 41 footnotes.
CONFIDENCE STANDARD	ICD 203. Confidence is stated separately from likelihood.
COMPANION PAPERS	Paper I, <i>Not Science Fiction</i> ; Paper III, <i>The Adjacent-Launch Seam</i>
CLASSIFICATION	Unclassified // Open source

Abstract

Small unmanned aircraft systems have matured into precision weapons capable of threatening political leadership; the companion Paper I establishes that capability as real and proliferating. This paper — the second in a series — asks whether any state can reliably defend against it. It argues that terminal defense against low, slow, small drones over populated areas is a structural gap common to states across regime types: a close-in launch reliably leaves the defender less warning time than its detect-classify-decide-engage loop requires, no state has shown that it can compress that loop enough, and the gap is a property of the problem — the physics of detecting small low targets, compressed decision timelines, the shift to non-emitting autonomous and fiber-optic control, and the collateral-damage limits on kinetic defeat in cities — rather than of any nation’s law, budget, or competence. The paper takes the People’s Republic of China as its anchor case precisely because China has built the most complete publicly documented prevention-and-authority regime — unified militarized command, mandatory manufacturer-level geofencing, and citywide prohibitions on drone sales, rentals, and entry — and yet is no more able to close the terminal column, as the June 2026 crash of a light aircraft into Beijing’s tallest building, within tightly controlled capital airspace and without interception, illustrates. Russia’s wartime experience supplies the capability-ceiling dataset: a large military under permissive rules of engagement could not stop drones launched from inside its own defended zone, while Ukraine’s high interception rates against long-range one-way-attack drones show that terminal defense succeeds when warning time is available. The paper

¹. Collin George, Founder, Sanctir LLC. This is a working paper and does not constitute, and should not be cited as, official U.S. Government analysis. It is Paper II in the series *Drone Threats to Political Leadership: Capability, Defense, and Authority*. All sources are open-source; citations follow The Bluebook: A Uniform System of Citation (21st ed.). The author welcomes correspondence.

distinguishes the tractable columns of the defensive chain — prevention and detection, which are national choices — from the intractable one, terminal hard-kill, and concludes that meaningful risk reduction lives left of launch.

IF YOU READ NOTHING ELSE

Thesis: Terminal defense against low, slow, small drones over populated areas is a structural gap common to states across regime types: a close-in launch reliably leaves less warning time than the defender's detect-classify-decide-engage loop requires, and no state has shown that it can compress that loop enough.

Prevention and detection are national choices; terminal hard-kill is roughly invariant.

The terminal-mitigation column is not reliably solved by any state in the close-in case, where warning time falls below the defender's detect-classify-decide-engage loop; it is bounded by physics, decision latency, and collateral limits rather than by authority or budget.

Russia — a large military under permissive ROE — could not stop drones launched from inside its own defended zone; its resort to mass mobile-internet shutdowns concedes the terminal gap. Ukraine's high interception rates against long-range one-way-attack drones show that the column's limit is warning time.

1. Introduction

Small unmanned aircraft systems (sUAS) have matured into precision weapons capable of threatening political leadership. The first paper in this series establishes that capability as real, fielded, and proliferating rather than speculative;² this paper takes the capability as given and asks a different question: can any state reliably defend against it? The answer, on the open-source evidence, is that the decisive phase of defense — terminal interdiction over populated areas — is not reliably solved by anyone, and that this is a property of the problem rather than of any nation's law, budget, or competence.

THESIS

Terminal defense against low, slow, small drones over populated areas is a structural gap common to states across regime types. Two claims carry the argument. First, a close-in launch over a populated area reliably leaves the defender less warning time than its detect-classify-decide-engage loop requires. Second, no state has shown that it can compress that loop enough to recover the engagement, because the binding limits are physics, identification, and collateral risk rather than authority or budget. The defensive chain has three columns — prevention, detection, and terminal mitigation. The first two are national choices and vary widely by regime; the third is roughly invariant across states. Because the terminal column cannot be relied upon in the close-in case anywhere, meaningful risk reduction depends on the columns that can be chosen — prevention and detection, left of launch (**high confidence**).

2. Collin George, *Not Science Fiction: The Maturation of Small-UAS as a Precision Weapon* (Drone Threats to Political Leadership, Paper I) (forthcoming 2026) (establishing the capability as mature, fielded, and proliferating). Capability claims in this paper are cited to Paper I rather than re-proved here.

The paper takes the People's Republic of China as its anchor case for a specific reason: China has built the most complete publicly documented prevention-and-authority regime — unified militarized command over capital security, mandatory manufacturer-level geofencing, and citywide prohibitions on drone sales, rentals, and entry — and is nonetheless no more able to close the terminal column than states that have adopted none of these measures. China is therefore not a model to emulate but an upper-bound test: if the most authority-maximal, surveillance-permissive regime on earth cannot close the terminal gap, the gap is structural. Russia's wartime experience supplies the complementary test, the capability ceiling — a large military operating under permissive rules of engagement that could not stop small drones launched from inside its own defended zone.

The argument bears directly on U.S. policy, developed in the third paper of this series, which identifies the specific statutory and coordination seams in National Capital Region leadership protection.³ If terminal interdiction is structurally unreliable, the U.S. policy question is not how to acquire a decisive interdiction capability that does not exist, but how to invest in the left-of-launch columns within constitutional constraints. Part 2 states scope and method; Part 3 positions the contribution; Part 4 defines the three-column framework; Parts 5–7 develop the anchor case, the capability ceiling, and the broader incident record; Part 8 explains why the terminal column is structurally hard; Parts 9–12 present findings, implications, limitations, and conclusion.

2. Scope, Method, and Sources

Scope. This paper assesses the effectiveness and limits of counter-UAS defense against small drones threatening political leadership, comparatively across regime types. It is a defensive effectiveness assessment. It does not assess, and does not contain, attack methodology, targeting, tradecraft, or means of defeating specific defenses; where the mechanics of an engagement appear, they appear only as constraints on the defender.

Threat model. The series addresses one threat class — small unmanned aircraft operating at low altitude and short standoff against protected persons and sites. Paper I establishes the capability as it exists globally; this paper addresses the defender's problem against low, slow, small platforms over populated areas; and Paper III addresses the lone domestic actor launching close-in from private property near a protected site in the National Capital Region. The variable that joins them is warning time: Paper I shows that the capability compresses it, this paper shows that terminal defense fails when it collapses, and Paper III shows where U.S. law leaves it collapsed.

Method. The paper decomposes defense into three columns — prevention (reducing the population of viable platforms and launch positions), detection (achieving warning time and identification), and terminal mitigation (physically defeating a threat in its final phase) — and evaluates each across states. It uses China as an anchor (maximal case), Russia-Ukraine as the largest real-world dataset (capability ceiling), and the cross-national incident record as corroboration.

3. Collin George, *The Adjacent-Launch Seam: Counter-UAS Authority Gaps in the National Capital Region* (Drone Threats to Political Leadership, Paper III) (forthcoming 2026) (applying the structural finding to U.S. statutory seams).

Sources and estimative language. The analysis rests exclusively on open-source materials — government and military documents, GAO and CRS products, established think-tank analysis, technical literature, and reputable reporting. It contains no classified information. Source types are labeled where it matters: government doctrine, belligerent claim, manufacturer claim, sensor-network dataset, interview-based estimate, and vendor marketing are not treated as equivalent. Confidence levels follow ICD 203 and are stated separately from likelihood.⁴

3. Prior Literature and Contribution

The prevention/detection/mitigation decomposition this paper uses is not itself new: it is standard in the technical counter-UAS literature and in institutional doctrine, including the 2026 Joint Interagency Task Force 401 handbook and its “Five Ds” framework.⁵ The comparative China literature is also well developed, but it treats China either as a model of decisive state capacity to emulate or as a threat to counter. Neither the taxonomy literature nor the China literature has drawn the two distinctions on which this paper turns.

This paper’s contribution is therefore narrow and specific. First, it argues that of the three columns, prevention and detection are regime-variable policy choices while terminal mitigation is bounded by physics, decision latency, and collateral limits and is thus roughly invariant across states — a distinction the existing taxonomy does not draw — and it identifies warning time as the variable that determines whether the terminal column can be exercised at all. Second, it reframes China from model or threat into an analytic upper-bound test: because China operates the most complete publicly documented prevention-and-authority regime, its inability to close the terminal column shows the gap is structural rather than a function of any state’s competence. Third, it connects the comparative finding to the U.S. statutory analysis in the companion paper.

4. The Defensive Chain: Three Columns

Defense against a small-UAS threat to a fixed, high-value site divides into three sequential columns, each with a different tractability profile.

Prevention reduces the population of viable platforms and launch positions before any flight: manufacturer-level geofencing, real-name registration, supply-chain and transport controls, airspace

4. Intelligence Community Directive 203, Analytic Standards (ODNI, Jan. 2, 2015). Analyst confidence (source quality) and likelihood are stated separately and not combined within a single expression.

5. On the prevention/detection/mitigation taxonomy this paper adopts and extends, see Joint Interagency Task Force 401, Small Drones, Big Problems: A First Principles Approach to Countering-UAS (Dep’t of Def. [styled Dep’t of War], June 18, 2026) (released July 8, 2026) (the “Five Ds”); and C-UAS technical surveys, e.g., Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges and Future Trends, arXiv:2008.12461, together with the homeland-security “left-of-launch” literature. On the comparative China dimension — which treats China as a model to emulate or a threat to counter — see Mina Marcus, China’s Conceptual Approaches to Counter-UAS and Lessons Drawn From Recent Conflicts (CASI, Air Univ., Apr. 2025); Ctr. for a New Am. Sec., Countering the Swarm and Swarms over the Strait; Atlantic Council, A Global Strategy to Secure UAS Supply Chains; and Mercatus Ctr., Drone Policy and Industrial Policy in the United States and China. Also U.S. Gov’t Accountability Off., GAO-22-105705 (Mar. 2022); Cong. Rsch. Serv., R48477 (2025).

restriction, and physical-security screening of launch positions. Prevention is a national policy choice and varies enormously by regime; it is the column where state capacity and legal latitude matter most.

Detection achieves warning time and identification once a platform is airborne: layered radar, radio-frequency, electro-optical/infrared, and acoustic sensing fused into a common picture. Detection is partly tractable but degrades sharply against the non-emitting autonomous and fiber-optic platforms whose existence Paper I documents;⁶ against a platform that neither transmits nor listens, the mature radio-frequency detection layer contributes little.

Terminal mitigation physically defeats the threat in its final phase. This column is bounded not by law or budget but by physics, decision latency, and collateral-damage limits over populated areas (Part 8). It is roughly invariant across states: the constraints that make it hard in Washington make it hard in Beijing and Moscow. Terminal mitigation is not impossible in general — Ukraine reports intercepting the large majority of long-range one-way-attack drones (Part 6) — but it depends on warning time, and the constraints in Part 8 remove that time in the close-in, low-altitude, populated-area case this series addresses. The central claim of this paper is that the first two columns are where national choices move risk, and the third is where every state, regardless of regime, is left with an unsolved residual.

5. The Anchor Case: The People's Republic of China

China is the maximal case on the two tractable columns. If its terminal column nonetheless remains open, the structural claim follows a fortiori.

5.1 Unified command

Leadership protection in Beijing is a single, party-controlled, militarized chain running from the CCP General Office and Central Military Commission through the Central Guard Bureau and its close-protection unit, backed by the Ministry of Public Security, the People's Armed Police Beijing Corps, and the PLA Beijing Garrison.^{7 8} There is no Chinese analogue to the U.S. inter-agency seam among the Secret Service, DHS, DOJ, the FAA, the Capitol Police, and the National Guard, and no Posse Comitatus constraint barring military forces from domestic policing. On the authority axis, China has removed every seam the U.S. framework leaves open.

5.2 The prevention regime

China's prevention column is the most complete publicly documented. The Interim Regulations on the Administration of Unmanned Aircraft Flight, effective 1 January 2024, impose real-name registration, operator licensing, controlled and restricted airspace, and mandatory operational identification.⁹ Beijing

⁶. Supra note 2.

⁷. On the Central Guard Bureau (中央警卫局) and the Central Guard Unit (PLA Unit 61889, formerly the 8341 Unit), open-source detail is secondary and partly dated; organizational specifics are attested in outline but uncertain in current detail. Protection runs from the CCP General Office and Central Military Commission through the CGB.

⁸. Capital security is layered across the CGB, the Ministry of Public Security, the People's Armed Police Beijing Corps, and the PLA Beijing Garrison, all answering ultimately to the Central Military Commission. There is no PRC analogue to the U.S. inter-agency authority seam or to the Posse Comitatus Act (18 U.S.C. § 1385).

designated its entire administrative region controlled airspace for unmanned aircraft in August 2025, requiring approval for any flight, and, effective 1 May 2026, prohibited the sale or rental of drones and seventeen categories of core components to buyers in the city, prohibited transporting or carrying them into the city (excepting existing, real-name-registered and verified drones carried by their owners), and barred new storage sites citywide and any storage site inside the Sixth Ring Road, defining a storage site as more than three drones or ten core components at one address — extending control from flight to acquisition and possession. The regime tightened further after the June 2026 CITIC Tower crash: a permanent restricted zone of more than 280,000 square kilometers around the capital, within which general-aviation flights require approval, took effect on 20 September 2026, and revised municipal rules effective 15 November 2026 prohibit possession and storage of drones and core components throughout Beijing’s administrative area.¹⁰ Most consequentially, China mandates at the manufacturer and firmware level what the United States leaves voluntary: on the available evidence DJI’s China-market units operate under enforced geofencing and forced registration, even as it removed automatic no-fly-zone enforcement in the United States in January 2025.¹¹ The same manufacturer that disabled its U.S. safety geofences is compelled to enforce them at home.

5.3 The counter-UAS industrial base

China’s counter-drone industrial base is large and state-linked, spanning radio-frequency detection, jamming and spoofing, directed energy, and integrated command systems, with more than three thousand manufacturers and rapidly rising government procurement.¹² On the prevention and detection columns, in other words, China has built at scale.

9. Interim Regulations on the Administration of Unmanned Aircraft Flight (无人驾驶航空器飞行管理暂行条例) (State Council & Cent. Mil. Comm’n, issued May 31, 2023; eff. Jan. 1, 2024) (real-name registration, operator licensing, controlled/restricted airspace, operational identification, penalties).

10. Beijing Municipal notice designating the entire administrative region controlled airspace (管制空域) for unmanned aircraft (Aug. 3, 2025; published Aug. 4, 2025) (officials described the notice as restating existing policy); Beijing Municipal Provisions on the Administration of Unmanned Aircraft (北京市无人驾驶航空器管理规定) (adopted Mar. 27, 2026; eff. May 1, 2026) (prohibiting sale or rental of drones and 17 core components to buyers in Beijing; prohibiting transport or carriage of drones and core components into the city, except existing real-name-registered and verified drones carried by their owners; barring new storage sites citywide and any storage site inside the Sixth Ring Road, a storage site being more than three drones or ten core components at one address; and prohibiting agricultural and forestry drone operations inside the Sixth Ring Road). See Standing Comm. of the Beijing Mun. People’s Cong., explanatory release (bjrd.gov.cn, Apr. 10, 2026). These are administrative prohibitions under municipal regulation, not criminal offenses. On the post-crash tightening, see Caixin Global, Digitimes, and DroneXL reporting of Sept. 13–21, 2026 (possession and storage ban effective Nov. 15, 2026, with buyback and disposal channels; permanent restricted airspace of more than 280,000 km² within roughly 300 km of Beijing effective Sept. 20, 2026).

11. DJI’s China-market units operate under enforced geofencing covering Beijing and mandatory CAAC real-name registration (an inference from geofence coverage and CAAC rules; DJI publishes no market-by-market statement); by contrast it removed automatic no-fly-zone enforcement in the United States on Jan. 13, 2025 (converting “Restricted Zones” to advisory “Enhanced Warning Zones”) and extended the change to all remaining international markets on Nov. 17, 2025 (having done so in the EU in Jan. 2024). Separately, on Dec. 22, 2025 the FCC added all foreign-produced UAS and critical components, including DJI’s, to its Covered List, barring new equipment authorizations but leaving previously authorized models in use; a Jan. 7, 2026 Public Notice exempted Blue UAS Cleared List items and qualifying domestic end products through Jan. 1, 2027 and opened a conditional-approval path, and DJI challenged its designation in Feb. 2026. The U.S. FAA does not mandate manufacturer geofencing. The asymmetry is the analytic point: China imposes mandatory hard geofencing on the same manufacturer that removed it in the U.S.

12. Tye Graham & Peter W. Singer, China’s counter-UAV efforts reveal more than technological advancement, *Defense One* (May 2, 2025) (reporting more than 3,000 anti-drone manufacturers and rising government procurement notices — 87 (2022), 122 (2023), 205 (2024)). On directed energy, see open reporting on the Poly Technologies “Silent Hunter” laser and CETC integrated systems (vendor/marketing sourcing; treat capability claims as promotional).

5.4 The terminal test

Yet the terminal column remains open. On 26 June 2026 a light aircraft departed its expected route within Beijing's tightly controlled capital airspace and struck the CITIC Tower — the capital's tallest building, in its central business district — weeks after the citywide drone rules took effect, and no interception was reported.¹³ Whether interception was technically impossible or was withheld to avoid collateral damage over a dense urban core, the outcome is identical for the analysis: terminal interdiction did not occur, in the airspace of the state that has done the most to prevent exactly this. Because the aircraft was transponder-equipped and tracked, the case bears on decision latency and collateral limits more than on detection. The institutional picture is consistent. The most authoritative open assessment finds that PLA counter-UAS doctrine and integrated command-and-control remain immature and that urban counter-UAS is a particular weakness;¹⁴ Western open-source analysis of Chinese exercises reports a neutralization rate near forty percent, a figure that is unofficial and contested but points the same direction.¹⁵ China has closed the authority and prevention seams and still cannot guarantee the terminal engagement (**moderate confidence: the point rests on an analogy, on unofficial figures, and on doctrinal assessments of an opaque system**).

6. The Capability Ceiling: Russia and Ukraine

If China is the maximal defender on the tractable columns, the Russia-Ukraine war is the largest real-world test of terminal defense under the most permissive conditions imaginable — a large military, combat-experienced, operating under wartime rules of engagement with far fewer collateral constraints than apply in a peacetime capital. The record is the strongest available evidence that the terminal column is unsolved even when every legal and political limit is removed.

Ukraine's June 2025 deep-strike operation smuggled roughly 117 short-range attack drones into Russia and launched them from concealment near five strategic airbases, defeating an outward-oriented air-defense system by collapsing warning time to near zero from within the defended zone.¹⁶ The drones were controlled over Russia's own commercial mobile networks rather than by fiber; what defeated the defense was not signal immunity but the absence of warning time and the failure of prevention and detection inside the defended zone. The precise battle-damage figures are disputed — Ukraine's belligerent claim of forty-one aircraft hit exceeds independent estimates of roughly ten to thirteen

^{13.} See, e.g., Reuters, CNN, and South China Morning Post reporting, June 26–27, 2026 (a Sunward SA 60L Aurora light aircraft struck the CITIC Tower, Beijing's tallest building, killing the pilot and injuring 13; the aircraft (registration B-12PP) deviated from its expected route within tightly controlled airspace, and, per flight-tracking data cited in press reports, its ADS-B transmissions ended shortly before impact near the East Third Ring Road; the suggestion that it could have reached Zhongnanhai is an analyst's counterfactual, not a reported fact). No source reports an attempted interception; whether interception was impossible or withheld for collateral reasons is not established. The incident involves a manned light aircraft, not a drone, and is used as an analogy for terminal engagement of a low, slow contact over the urban core.

^{14.} Marcus, *supra* note 5 (open-source; the PLA “lacks a set of specialized doctrine” for countering UAS; “[c]ore command and control systems to coordinate various counter-UAS weapons and equipment are also lacking”; counter-UAS technologies for urban areas are “still immature”; low-slow-small targets are “difficult to detect and attack”). The last two assessments are CASI's reports of PRC sources: People's Armed Police engineers writing in 2022 and a PLA unit writing in 2018, respectively.

^{15.} Graham & Singer, *supra* note 12 (Western open-source analysis of Chinese media reporting that PLA countermeasures “neutralize[d] only around 40 percent of incoming UAVs” in summer 2024 exercises). The figure is unofficial, its exercise conditions are unknown, and it has not been independently vetted; treat as illustrative, not definitive.

destroyed — but the disputed number is the effect, not the fact of penetration, which is not in doubt. Fiber-optic control, a separate development at the front, compounds the problem: because such drones neither transmit nor receive radio-frequency signals, they are immune to the jamming and RF detection on which most fixed-site defense relies, and they are now produced at industrial scale.¹⁷ On the offense side of the same exchange, autonomy raises the attacker’s success rate sharply: an interview-based CSIS assessment estimates that autonomous terminal navigation lifts engagement success from the range of ten-to-twenty percent to seventy-to-eighty percent, though the same source cautions that only a small fraction of fielded drones yet use such guidance.¹⁸ Russia’s response is itself the tell: unable to rely on terminal defeat, it has resorted to mass mobile-internet shutdowns as a prevention measure — a costly, population-wide left-of-launch step that concedes the terminal column is not dependable.¹⁹

The same war supplies the counter-case, and it sharpens rather than weakens the thesis. Ukraine’s Ministry of Defence reported intercepting about 90 percent of the Shahed-type and other long-range attack drones launched in March 2026 — 5,833 of 6,463 by its count, a tally that in Ukrainian practice combines kinetic interceptions with electronic-warfare suppressions — and Ukraine’s Air Force attributes roughly one in three downings to low-cost interceptor drones.²⁰ Terminal defense works against these threats because they are large, long-range, and observable for tens of minutes on approach: the defender has time to detect, classify, decide, and engage. Spiderweb and the close-access cases in Part 7 succeed for the opposite reason. The variable that separates success from failure in the terminal column is warning time, and the close-in launch is what removes it.

^{16.} Security Service of Ukraine (SBU) / General Staff statements, June 1–3, 2025 (claiming 117 FPV drones, smuggled into Russia and launched from concealed truck compartments, struck five strategic airbases and hit 41 aircraft) — a belligerent claim. Independent estimates are lower: a senior NATO official, via Meduza, put confirmed aircraft destroyed at roughly 10–13 of ~40 damaged; U.S. officials estimated roughly 20 hit and about 10 destroyed. The drones were controlled over Russian commercial mobile networks, not by fiber-optic link. Five bases were targeted (Belaya, Dyagilevo, Ivanovo Severny, Olenya, Ukrainka); the Ukrainka strike reportedly failed, so four were effectively struck.

^{17.} On fiber-optic control as immune to radio-frequency jamming and detection, and its industrial scale, see Paper I, supra note 2, and Inst. for the Study of War (Sept. 2025), citing Ushkuynik director Alexey Chadayev via RBC-Ukraine (a manufacturer/state-adjacent claim of 50,000+ fiber-optic FPVs per month; unaudited). NATO Allied Command Transformation, Innovation Challenge 2025/June: Countering Fiber-Optic-Controlled FPV Drones (May 2025), states that “EW counter-UAS systems are ineffective against this type of drone.”

^{18.} Kateryna Bondar, Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare (CSIS, Mar. 6, 2025) (interview-based; estimating that autonomous navigation raises target-engagement success from ~10–20% to ~70–80% and can reduce drones-per-target from eight or nine to one or two — while noting that Ukraine began procuring ~10,000 AI-enhanced drones in 2024 against ~2 million drones produced, and that the field is “very far from killer robots”). Cited for the offense-side effectiveness trend, not as a measured kill-chain study.

^{19.} On Russia’s resort to mass mobile-internet shutdowns as a drone countermeasure, see The Moscow Times (July 15, 2025), citing the watchdog Na Svyazi (655 shutdowns in June 2025 alone); the figure has since been exceeded — The Insider reported at least 1,470 shutdowns in July 2025, and The Moscow Times (Mar. 10, 2026) reported Na Svyazi’s finding that restrictions were being introduced daily in an average of 63 regions. An extreme, economically costly prevention measure that underscores the weakness of terminal options.

^{20.} George Allison, Ukraine claims over 90 percent drone interception rate, *UK Defence Journal* (Apr. 16, 2026) (Ukrainian Ministry of Defence figures for March 2026: 5,833 of 6,463 Shahed-type and other drones intercepted); Novel interceptor drones bend air-defense economics in Ukraine’s favor, *Defense News* (Mar. 5, 2026). Ministry figures are belligerent claims and are cited for direction, not precision.

7. The Broader Record: Democracies and Others

The cross-national incident record shows drones and small aircraft reaching protected leadership and sensitive sites under both democratic and authoritarian security models — evidence that the gap is not confined to any regime type. A commercial quadcopter reached the White House South Lawn in 2015;²¹ a small drone crashed near the German Chancellor at a 2013 campaign rally;²² explosive-laden commercial drones detonated near the Venezuelan president during a 2018 televised address;²³ drones reached the Kremlin's Senate dome in 2023 over the best-defended site in Russia;²⁴ a one-way-attack drone killed three U.S. soldiers at Tower 22 in Jordan in January 2024 after it was reportedly confused with a returning U.S. drone;²⁵ a drone launched from Lebanon struck the Israeli Prime Minister's residence in Caesarea in October 2024 despite one of the most capable integrated air defenses in the world;²⁶ and a sustained 2025–2026 wave of drone incursions repeatedly closed major European airports whose operators frequently could not even confirm the number or type of drones involved.²⁷ The recurring outcome across all of these is detection failure or delayed detection, and reliance on prevention, luck, or the incident's own limited intent rather than on successful terminal interception. Where terminal engagement did succeed — two of three drones over Baghdad in 2021, and electronic warfare over the Kremlin in 2023 — it succeeded late and only in part.

8. Why the Terminal Column Is Structurally Hard

The invariance of the terminal column across regimes is explained by a consistent set of constraints that no authority model changes. First, physics and clutter: small drones present radar cross-sections comparable to birds and fly at low altitudes where ground clutter dominates returns; their slow speeds fall within the clutter band and defeat moving-target-indication filtering; and urban multipath and obstruction

^{21.} A DJI Phantom quadcopter crashed on the White House South Lawn, Jan. 26, 2015; the Secret Service determined it posed no threat, and DJI subsequently pushed a firmware geofence around Washington — a manufacturer-side mitigation. See *White House Drone Operator Works at Intelligence Agency*, NPR (Jan. 27, 2015); *No Charges for Operator of Drone That Crashed at White House*, NPR (Mar. 18, 2015).

^{22.} A Parrot AR.Drone was flown over a CDU campaign rally in Dresden, Sept. 15, 2013, crashing in front of the stage near Chancellor Merkel and the Defense Minister in a protest stunt. See *Pirates Crash Protest Drone at Merkel Rally*, The Local (Sept. 16, 2013); *Watch the Pirate Party Fly a Drone in Front of Germany's Chancellor*, Wash. Post (Sept. 18, 2013).

^{23.} Explosive-laden DJI M600 drones detonated near Venezuelan President Maduro during a televised address, Aug. 4, 2018; intent and perpetrator remain debated, and some accounts attribute the event to a different cause. See *Venezuelan Officials Say President Nicolás Maduro Is Unharmed After Drone 'Attack'*, NPR (Aug. 4, 2018); *Venezuela's Nicolas Maduro Survives Drone 'Attack'*, Al Jazeera (Aug. 5, 2018).

^{24.} Two drones reached the Kremlin Senate dome, May 3, 2023; Russia attributed the downing to electronic-warfare systems and characterized the event as an attempted assassination. The drones reached the heart of Moscow before being disabled. See *Russia Accuses Ukraine of Attempt to Kill Putin with Drones*, Al Jazeera (May 3, 2023); *False Flag? Analysts Say Russia 'Likely Staged' Kremlin Drone Attack It Blamed on Ukraine and the West*, CNBC (May 4, 2023) (attribution contested).

^{25.} Enemy drone that killed American troops in Jordan was mistaken for a U.S. drone, preliminary report suggests, *PBS NewsHour* (Jan. 2024) (three U.S. Army Reserve soldiers killed, more than forty wounded). Cited for the identification failure, a decision-latency constraint (Part 8).

^{26.} See Paper I, supra note 2 (Caesarea, Oct. 19, 2024); Hezbollah drone targets Netanyahu's house in Caesarea; PM, wife not home, no injuries, *Times of Israel* (Oct. 19, 2024).

^{27.} Drone incursions closed Copenhagen and Oslo (Sept. 22, 2025), Munich (Oct. 2–3, 2025), and other European airports through 2025–2026; authorities frequently could not confirm the number or type of drones involved. See *Drone Sightings Disrupt Flights at Copenhagen, Oslo Airports*, Al Jazeera (Sept. 22, 2025); *Munich Airport Reopens After Latest European Drone Breach*, AeroTime (Oct. 3, 2025); *Fact-Checking Europe's 'Drone Problem': Why Are Airports Closing over Drone Sightings?*, Euronews (Nov. 20, 2025).

create shadow zones and false targets.^{28 29} Second, the shift to non-emitters: radio-frequency detection and jamming, the workhorse of most fixed-site defense, fail against autonomous and fiber-optic platforms.³⁰ Third, decision latency and identification: at operational speeds the defender must detect, classify, identify, and act within seconds, often with no reliable means of distinguishing a hostile drone from a bird, a hobbyist, or a media platform.³¹ Fourth, collateral limits: over populated areas, kinetic interception risks falling debris and secondary casualties, which is why the U.S. Department of Defense has repeatedly solicited low-collateral interceptors and defeat options for urban and sensitive-site use — an implicit admission that current kinetic options are unsuitable there.³² These constraints are the same in every capital. They are the reason the terminal column is a property of the problem, not of the defender **(high confidence)**.

Three responses are commonly offered to these constraints, and none removes them. Low-collateral interceptors — net capture, interceptor drones, and frangible or proximity-fused munitions — reduce debris risk and shorten the engagement step. High-power microwave defeats non-emitting platforms that jamming cannot, at the cost of its own collateral effects on nearby electronics. Pre-delegated engagement authority shortens the decision step. Each is worth acquiring. None shortens detection, classification, and identification, which is where the close-in case fails: an interceptor that is not cued in time does not launch, and authority delegated in advance cannot be exercised against a contact that has not been classified. The 2026 FIFA World Cup operations, in which federal authorities reported seizing more than 700 drones in restricted airspace across the eleven U.S. host cities, support this distinction rather than rebut it.³³ That result was achieved inside nearly 250 pre-declared temporary flight restrictions, with sensors and intercept teams positioned in advance — conditions of ample warning, and the prevention and detection columns working as designed. It does not test a non-emitting platform launched close-in without warning **(moderate confidence)**.

28. GAO-22-105705, supra note 5 (counter-drone systems have “limited ability to detect and track small UAS” and mitigation is often “only effective at around 1,000 feet or less”; birds and other objects can generate false detections).

29. On the physics: small-UAS radar cross-sections are often comparable to birds; low grazing angles are dominated by ground clutter; slow speeds fall within the clutter band and defeat moving-target-indication filtering; and urban multipath and obstruction create shadow zones and false targets. See Jian Wang, Yongxin Liu & Houbing Song, *Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends*, 36 IEEE Aerospace & Elec. Sys. Mag., no. 3, at 4–29 (Mar. 2021) (also arXiv:2008.12461, supra note 5) (surveying radar, RF, EO/IR, and acoustic detection of small UAS and their limits against low, slow, small targets in clutter).

30. NATO Allied Command Transformation, Innovation Challenge 2025/June: Countering Fiber-Optic-Controlled FPV Drones (May 2025): “The combination of high maneuverability, jamming immunity, and low visual and radar signature makes these drones particularly dangerous to frontline troops and forward elements.”

31. Cong. Rsch. Serv., R48477, supra note 5. On Aug. 28, 2025 DOD established Joint Interagency Task Force 401, disestablishing the Joint Counter-small UAS Office; DOD materials describe small UAS as “abundant and difficult to detect” and note their use of terrain masking and cluttered urban environments. Executive-branch documents issued since late 2025 style the Department as the “Department of War”; this paper uses the statutory name.

32. See Joint Counter-small UAS Office, Request for Information: Low Collateral Effects Interceptors (Jan. 19, 2021); Def. Innovation Unit, DIU, NORTHCOM, and JCO Announce Solicitation for Joint Low-Collateral Defeat (May 5, 2025). The repeated solicitation of low-collateral defeat options for domestic and sensitive-site use is an implicit acknowledgment that current kinetic options are unsuitable over populated areas.

33. Press Release, Fed. Aviation Admin., Successful Counter-Drone Efforts Helped Keep Millions of Fans Safe During FIFA World Cup 2026, With More Than 700 Drones Seized (July 22, 2026) (FBI and DHS seized more than 700 drones operating in restricted airspace across all 11 U.S. host cities; nearly 250 temporary flight restrictions; use of ground intercept teams). The release does not describe detection methods or report any non-emitting platform; that sensors were in place before the restricted periods is the author’s inference from the pre-declared restrictions.

9. Consolidated Findings

NO.	FINDING / JUDGMENT	ANALYST CONFIDENCE
T	Thesis: Terminal defense against low, slow, small drones over populated areas is a structural gap common to states across regime types: a close-in launch reliably leaves less warning time than the defender's detect-classify-decide-engage loop requires, and no state has shown that it can compress that loop enough. Prevention and detection are national choices; terminal hard-kill is roughly invariant.	High
F-1	The prevention column is tractable and varies by regime; China's is the most complete publicly documented (unified command, manufacturer geofencing, citywide sale-and-entry prohibitions).	High
F-2	The detection column is partly tractable but degrades sharply against non-emitting autonomous and fiber-optic platforms, which defeat the mature RF layer.	Moderate-High
F-3	The terminal-mitigation column is not reliably solved by any state in the close-in case, where warning time falls below the defender's detect-classify-decide-engage loop; it is bounded by physics, decision latency, and collateral limits rather than by authority or budget.	High
F-4	China — the maximal case on prevention and authority — still leaves the terminal column open, as the June 2026 CITIC Tower crash and CASI's immaturity findings indicate.	Moderate
F-5	Russia — a large military under permissive ROE — could not stop drones launched from inside its own defended zone; its resort to mass mobile-internet shutdowns concedes the terminal gap. Ukraine's high interception rates against long-range one-way-attack drones show that the column's limit is warning time.	High
F-6	The cross-national incident record (White House, Merkel, Maduro, Kremlin, Tower 22, Caesarea, European airports) shows drones reaching protected sites under both democratic and authoritarian models.	High (that incidents occurred); effects vary
F-7	Autonomy shifts the offense-defense exchange toward the attacker (interview-based estimates of sharply higher engagement success), reinforcing the priority of left-of-launch measures.	Moderate (interview-based)
F-8	Meaningful risk reduction lives in prevention and detection; terminal hard-kill is not a reliable procurement target for the close-in case in populated areas.	Moderate-High

Confidence levels reflect source quality under ICD 203 (supra note 4) and are stated separately from likelihood. Belligerent, manufacturer, and interview-based inputs are labeled as such and weighted accordingly.

10. Implications

The structural finding inverts the usual policy intuition. If the most authority-maximal state on earth cannot close the terminal column, then the answer to a leadership-protection gap is not to acquire more authority in pursuit of a decisive interdiction capability that does not exist. It is to invest in the columns that actually move risk — prevention and detection, left of launch — and to manage the irreducible terminal residual through hardening, evacuation, and rehearsed response.

For the United States, the corollary, developed in the companion paper, is favorable: prevention is what reduces risk, and prevention does not require the PRC's apparatus.³⁴ The United States can capture much of the achievable protection through constitutionally compatible prevention and detection measures — Remote-ID enforcement, reactivatable geo-awareness around a defined national-security site list, supply-chain investment in trusted platforms, and layered multi-sensor early detection — without importing the surveillance apparatus that makes China's prevention inseparable from repression.³⁵ The fragility of even voluntary prevention is a live risk: a single manufacturer removed automatic U.S. geofencing in 2025, and the FCC's December 2025 Covered List action will reshape the U.S. fleet only as the installed base turns over.³⁶ And the manned-aircraft analogy of the CITIC Tower is a caution against over-investing in terminal hard-kill: the collateral and decision-latency constraints that defeated engagement there are the same ones a small drone imposes.³⁷

11. Limitations and Scope Conditions

- **Opacity of the anchor case.** PRC internal-security arrangements are deliberately opaque; organizational and doctrinal specifics rest on secondary and sometimes dated open sources and are attested in outline rather than current detail.³⁸
- **The CITIC analogy.** The June 2026 incident involved a manned light aircraft, not a drone; it is used as an analogy for terminal engagement of a low, slow contact over the urban core, and no source establishes whether interception was impossible or withheld. The aircraft was transponder-equipped, so the case bears on decision latency and collateral limits more than on detection.³⁹
- **Contested figures.** The ~40% PLA neutralization figure is unofficial and contested;⁴⁰ battle-damage figures for the June 2025 deep strike are disputed; and production and inventory figures from the war are belligerent or manufacturer claims, labeled as such.

³⁴. Supra note 3.

³⁵. On the fragility of prevention layers, see supra note 11 (DJI's 2025 removal of automatic U.S. geofencing). On supply-chain concentration, DJI is estimated to hold roughly 80% of the U.S. commercial market and up to ~70% globally; see, e.g., Atlantic Council, A global strategy to secure UAS supply chains.

³⁶. Supra note 11 (FCC Covered List action of Dec. 22, 2025 and subsequent exemptions).

³⁷. Supra note 13 (CITIC Tower). The manned-aircraft analogy is imperfect but apposite: a slow contact over the dense urban core presents the same collateral-risk and decision-latency constraints that bound kinetic defeat of a small drone.

³⁸. Supra note 14 (CASI: PRC counter-UAS doctrine and integrated C2 remain immature; the PRC advantage analyzed here is legal-institutional, not necessarily technical-operational).

³⁹. Supra note 37.

⁴⁰. Supra note 15 (the ~40% figure is unofficial and contested).

- **Interview-based effectiveness.** The autonomy engagement-success estimates are interview-based, not a measured kill-chain study, and the same source notes limited current fielding of AI guidance.⁴¹
- **Non-transferability.** The PRC model's apparent effectiveness on prevention is inseparable from surveillance-state features that are legally and normatively non-transferable to the United States; this paper treats the prevention logic as transferable, not the apparatus.

12. Conclusion

The threat is real, as Paper I establishes; the question this paper answers is whether it can be stopped, and the answer is that its decisive phase cannot be reliably stopped by anyone once warning time collapses. The most complete publicly documented prevention-and-authority regime has not closed the terminal column, and the largest military tested against small drones in real combat has not closed it either. Because the gap is a property of the physics and the geometry rather than of any nation's institutions, the policy consequence is common to all states and specific in its direction: risk is reduced upstream, in prevention and detection, not at the moment of terminal engagement. The third paper in this series applies that conclusion to the United States. The through-line is complete: the capability is mature, no one can reliably defend against it at the terminal phase, and therefore the authority and investment choices that remain are the ones that matter.

Appendix A. Principal Sources

PRC framework and posture

- Interim Regulations on the Administration of Unmanned Aircraft Flight (eff. Jan. 1, 2024); Beijing controlled-airspace designation (Aug. 2025) and Beijing Municipal Provisions on the Administration of Unmanned Aircraft (eff. May 1, 2026).
- Mina Marcus, China's Conceptual Approaches to Counter-UAS (CASI, Air Univ., Apr. 2025).
- Tye Graham & Peter W. Singer, China's counter-UAV efforts reveal more than technological advancement, *Defense One* (May 2, 2025).
- Reporting on the June 26, 2026 CITIC Tower crash (Reuters; CNN; South China Morning Post; Newsweek).

Russia-Ukraine and technology

- SBU statements on the June 1, 2025 deep-strike operation (belligerent claims); independent estimates (NATO; U.S. officials).
- Inst. for the Study of War, citing Ushkuynik (Chadayeve) via RBC-Ukraine, on fiber-optic drone production (manufacturer claim); NATO ACT Innovation Challenge 2025/June (fiber-optic FPV drones); Ukrainian MoD interception data (UK Defence Journal; Defense News, Mar. 5, 2026).

⁴¹. Bondar, *supra* note 18.

- Kateryna Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare (CSIS, Mar. 6, 2025) (interview-based).

U.S. and comparative

- GAO-22-105705, Science & Tech Spotlight: Counter-Drone Technologies (Mar. 2022); Cong. Rsch. Serv., R48477, Department of Defense Counter-UAS (2025).
- Incident record: White House (2015); Dresden/Merkel (2013); Caracas/Maduro (2018); Kremlin (2023); Tower 22 (2024); Caesarea (2024); European airports (2025–2026).

Analytic standards

- Intelligence Community Directive 203, Analytic Standards (ODNI, Jan. 2, 2015).

Companion papers in this series

- George, C. Not Science Fiction: The Maturation of Small-UAS as a Precision Weapon (Paper I, forthcoming 2026).
- George, C. The Adjacent-Launch Seam: Counter-UAS Authority Gaps in the National Capital Region (Paper III, forthcoming 2026).

DISCLOSURE

Author's Statement on Sources and Independence

This paper was prepared in the author's personal capacity and is not official U.S. government analysis. It relies exclusively on publicly available sources, each cited. In the author's assessment it contains no classified information, no Controlled Unclassified Information, and no technical data or technology controlled under the ITAR or EAR; operational method, targeting, and build detail are deliberately omitted. The work was self-initiated and self-funded. No client, government, or foreign principal requested, directed, funded, or reviewed it. Inquiries: <https://sanctir.com/contact/>

ABOUT THE AUTHOR

Collin George is the founder of Sanctir LLC, where he advises on national security, export control, and compliance. He holds the CISSP. Correspondence: <https://sanctir.com/contact/>.

ORCID 0009-0007-8162-6839

SUGGESTED CITATION

Collin George, *The Terminal Residual: Warning Time and the Structural Limits of Small-UAS Defense*, Sanctir Working Paper WP-2026-D2 (2026-10-01), *Drone Threats to Political Leadership: Capability, Defense, and Authority*, Paper II, v1.6.

Keywords: counter-UAS; C-UAS; terminal defense; small unmanned aircraft systems; drones; leadership protection; China; People's Liberation Army; Russia-Ukraine war; fiber-optic drones; comparative security; homeland defense.