

Not Science Fiction:

The Maturation of Small-UAS as a Precision Weapon

Small-UAS strike capability is mature, commercially accessible, and already used against critical infrastructure and political leaders.

DOCUMENT	VERSION	DATE
WP-2026-D1	V1.6	2026-10-01
AUTHOR	ORGANIZATION	SERIES
COLLIN GEORGE	SANCTIR LLC	PAPER I 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 I of three — Not Science Fiction
DOCUMENT	WP-2026-D1 · v1.6 · 2026-10-01
SCOPE	Existence, maturity, and availability of small-UAS strike capability. Defensive effectiveness and legal analysis are reserved for Papers II and III.
SOURCES	Open source only. Bluebook (21st ed.) citations; 35 footnotes.
CONFIDENCE STANDARD	ICD 203. Confidence is stated separately from likelihood.
COMPANION PAPERS	Paper II, <i>The Terminal Residual</i> ; Paper III, <i>The Adjacent-Launch Seam</i>
CLASSIFICATION	Unclassified // Open source

Abstract

Skeptics dismiss the small-drone threat to political leadership as speculative — a capability that “will never happen” or that only an advanced state could field. This paper — the first in a series on drone threats to political leadership — refutes that view from the open record. It establishes that small unmanned aircraft systems have matured from hobbyist platforms into a precision weapon that is real, fielded, and widely proliferated. Three lines of evidence converge. First, the engineering is mature: autonomous and pre-programmed waypoint navigation, GPS-independent visual-inertial navigation, jam-resistant fiber-optic control, and onboard machine-vision terminal guidance are documented, in-production capabilities rather than laboratory concepts. Second, the capability is commercially accessible: strike-relevant platforms are available off the shelf or through low-cost assembly, defeating the claim that only a state industrial base could field them. Third, the cost and proliferation curves are steep and the open incident record is deep and global — weaponized commercial drones and one-way-attack munitions have reached critical infrastructure, military installations, and political leaders on multiple continents and are now produced at industrial scale in active conflict, and a lone-actor drone plot against the U.S. power grid has been prosecuted to a guilty plea. The paper is deliberately confined to existence, maturity, and availability; the effectiveness of defenses against this weapon, and the specific U.S. legal seams it exposes, are treated in the companion papers. The conclusion is narrow and firm: the threat object is not science fiction.

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 I 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.

IF YOU READ NOTHING ELSE

Master finding: Small-UAS strike capability is mature, commercially accessible, and already used against critical infrastructure and political leaders — not speculative, and not state-exclusive.

Strike-relevant capability is available off the shelf or through low-cost assembly; no advanced-state industrial base is required.

The open incident record shows weaponized drones reaching critical infrastructure, military installations, and political leaders or their residences on multiple continents, and a lone-actor drone plot prosecuted in the United States.

1. Introduction

The most common objection to taking the small-drone threat to political leadership seriously is that it is speculative — that a precision drone strike on a protected person is science fiction, or that only an advanced state could assemble such a capability. This paper refutes both claims from the open record. Its single job is to establish that the threat object is real: that small unmanned aircraft systems (sUAS) have matured from hobbyist platforms into a precision weapon that is fielded, commercially accessible, and widely proliferated.

CLAIM

Small-UAS strike capability is mature, commercially accessible, and already used against critical infrastructure and political leaders. The enabling technologies — autonomous navigation, GPS-independent navigation, jam-resistant fiber-optic control, and onboard machine-vision terminal guidance — are documented, in-production capabilities, not laboratory concepts, and meaningful capability is available off the shelf or through low-cost assembly. The claim of this paper is confined to existence, maturity, and availability (**high confidence**).

Scope discipline is essential to the argument. This paper deliberately does not assess how well defenses stop this weapon — that is the subject of the second paper in the series² — and it does not analyze the U.S. legal seams the weapon exposes, which are the subject of the third.³ It contains no employment method, targeting, tradecraft, or build instructions. The incident record below is used strictly as existence proof — evidence that the capability is real and has been used — not as an analysis of engagement outcomes. Keeping that line sharp is what makes the maturity claim defensible: a skeptic can dispute how lethal or how stoppable the weapon is, but not that it exists.

The paper is organized around three evidentiary buckets. Part 4 traces the engineering evolution to the present. Part 5 documents the commercial-off-the-shelf and one-way-attack baseline. Part 6 sets out the

2. Collin George, *The Terminal Residual: Warning Time and the Structural Limits of Small-UAS Defense* (Drone Threats to Political Leadership, Paper II) (forthcoming 2026) (assessing the effectiveness of defenses against the capability established here). Effectiveness of both attack and defense is reserved for Paper II; this paper establishes existence and maturity only.

cost and proliferation curves and the open incident record. Parts 2 and 3 state method and position the contribution; Parts 7–10 present findings, implications, limitations, and conclusion.

2. Scope, Method, and Sources

Scope. This paper establishes existence, maturity, and availability of small-UAS strike capability. It excludes, by design, defensive effectiveness (Paper II), legal-authority analysis (Paper III), and any operational method, targeting, tradecraft, weaponization, or build detail.

Threat model. The series addresses one threat class — small unmanned aircraft operating at low altitude and short standoff against protected persons and sites — and each paper emphasizes a different variant: this paper, the capability as it exists globally; Paper II, the defender’s problem against low, slow, small platforms over populated areas; and Paper III, 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. This paper shows that the capability compresses it; Paper II shows that terminal defense fails when it collapses; and Paper III shows where U.S. law leaves it collapsed.

Method. The paper assesses capability at the class level rather than by named platform, because the enabling technologies are commoditized and diffuse faster than any single model. It organizes evidence into three buckets — engineering evolution, the commercial and one-way-attack baseline, and the cost/proliferation curve plus the incident record — and applies a consistent rule to the incident record: each case ends with a single statement of what it proves about existence, and nothing more.

Sources and estimative language. Evidence is drawn from peer-reviewed robotics literature, OEM specifications, defense-market analysis, government and FFRDC products, and conflict reporting. Source types are labeled and not treated as equivalent: a peer-reviewed navigation study, an OEM datasheet, a market-research projection, a belligerent production claim, and a manufacturer capacity claim carry different weight, and the text says which is which. Confidence levels follow ICD 203.⁴

3. Prior Literature and Contribution

Writing on the drone threat tends to divide between sensationalism, which asserts danger without a disciplined evidence base, and dismissal, which treats the threat as hobbyist or futuristic. A substantial non-state-actor drone-terrorism literature documents weaponized-drone use by groups such as the Islamic State and, more recently, criminal organizations, and a growing institutional literature — including the 2026 Joint Interagency Task Force 401 handbook — frames the counter-UAS problem; but the technology-diffusion and defense-market literatures separately document navigation capability and production volumes and rarely assemble them into a single existence-and-maturity case aimed at the

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 threat to U.S. statutory seams).

4. Intelligence Community Directive 203, Analytic Standards (ODNI, Jan. 2, 2015). Source types (peer-reviewed, government, defense-market, OEM specification, belligerent claim, manufacturer claim, and conflict reporting) are labeled where it matters and are not treated as equivalent.

skeptic.⁵ This paper’s contribution is that assembly: a source-labeled, class-level maturity-and-proliferation record that deliberately separates existence (its subject) from effectiveness and employment (reserved for the companion papers), so that the core claim — the weapon is real and available — rests only on evidence a skeptic cannot dismiss as speculative or state-exclusive.

4. Engineering Evolution to the Present

4.1 Commodity autonomy

Autonomous flight entered the consumer class more than a decade ago. Waypoint planning, follow-me, and geofencing were features of recreational platforms by around 2014, and by March 2016 the DJI Phantom 4 was among the first mass-market consumer drones to actively avoid obstacles using dedicated cameras and to recognize and track a designated subject through machine vision.⁶ These are mass-market, no-expertise-required capabilities — the baseline from which everything since has advanced.

4.2 GPS-independent navigation

Navigation without satellite positioning is mature. Visual-inertial odometry fuses camera and inertial data to estimate a platform’s position in three dimensions without GNSS, and the technique is validated in the peer-reviewed robotics literature.⁷ It is moving into defense programs: a commercial visual-navigation package was demonstrated on a U.S. Army-accepted airframe with roughly seven meters of mean error over a 2.7-kilometer course — a demonstration, not fielded inventory, but a documented capability rather than a concept.⁸

4.3 From radio link toward autonomy and fiber-optic control

The historic vulnerability of a small drone — a jammable, detectable radio link — is being engineered out two ways. Fiber-optic control unspools a thin optical fiber that carries control and video as pulses of light, emitting no radio frequency and therefore immune to RF jamming and detection, with maximum distance

5. The “drone threat” literature tends to divide between sensationalism and dismissal; the technology-diffusion and defense-market literatures document capability and production but rarely assemble a disciplined existence-and-maturity case. On the non-state-actor drone-terrorism record, see Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (Combating Terrorism Ctr. at West Point, July 2018); Jake Dulligan et al., *The Rising Threat of Non-State Actor Commercial Drone Use: Emerging Capabilities and Threats*, CTC Sentinel, vol. 18, no. 3 (Mar. 2025). On the institutional counter-UAS framing, 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). This paper draws on peer-reviewed robotics sources, OEM specifications, defense-market analysis, and government/FFRDC products (CRS; CSIS; CTC; NCITE).

6. Product history: consumer waypoint planning, follow-me, and geofencing appeared c. 2014 (e.g., 3DR Iris+); the DJI Phantom 4 (announced Mar. 1, 2016) was among the first mass-market consumer drones to actively avoid obstacles via dedicated cameras (Yuneec’s Typhoon H, announced Jan. 2016, offered obstacle avoidance in its Intel RealSense-equipped configuration) and to track a designated subject (ActiveTrack) using machine vision.

7. Peer-review anchor for GPS-independent navigation: N. Gyagenda et al., *A Review of GNSS-Independent UAV Navigation Techniques*, 152 *Robotics & Autonomous Sys.* 104069 (2022). Visual-inertial odometry fuses camera and inertial data to estimate position without GNSS.

8. Red Cat and Palantir demonstrated visual-navigation software (“VNav”) on a U.S. Army-accepted Black Widow airframe — described by the companies as the first known commercial demonstration of visual navigation on a drone already accepted into a U.S. Army program, with a company-reported mean error of roughly 7 m over a 2.7 km route. See *Red Cat Proves Drone Software for GPS-Denied Navigation*, GPS World (Nov. 20, 2025). A demonstration, not fielded inventory.

capped by the length of cable on the spool.⁹ In parallel, onboard machine-vision terminal-guidance modules are in serial production, allowing a platform to hold a designated target through the final approach; on the best open accounting these are fielded in limited numbers relative to total drone output.¹⁰ The salient maturity fact for this paper is simply that non-emitting control and onboard guidance exist and are in production; what they imply for the defender is the subject of Paper II.¹¹

For a domestic actor, the operative non-emitting mode is neither fiber nor onboard AI but pre-programmed waypoint flight — a consumer capability mature for more than a decade (Part 4.1), in which a platform flies a stored route to a stored point with no command link required in its terminal phase. Fiber-optic control and onboard terminal guidance are conflict-zone developments that will widen the defender's problem as they diffuse (Part 8); waypoint autonomy is the non-emitting baseline available now. That distinction is the shared premise on which Papers II and III rest their detection analysis.

4.4 Payload and machine-vision milestones

Commercial payload capacity has climbed from camera-carrying multirotors to 40–50 kg agricultural sprayers to roughly 200 kg heavy-lift transport drones, and automated object recognition and tracking now run on embedded silicon.¹² Payload capacity is a maturity indicator, not weaponization; it is cited here only to show that the lift and the onboard autonomy exist as commodity engineering.

5. The Commercial and One-Way-Attack Baseline

5.1 Mainstream commercial classes

The commercial baseline is high and concentrated. In the Dedrone (Axon) 2025 detection data — drawn from the vendor's Europe–Middle East–Asia sensor network rather than a global census — DJI platforms accounted for approximately 83.5% of all drone detections and do-it-yourself builds — home-assembled platforms, including some FPV kits — approximately 9.8%, the latter a roughly 4.3× rise over the prior year in a partial-year dataset.¹³ The rising-DIY trend is the more telling figure: capability is diffusing away from a single regulated manufacturer toward assembled platforms that honor no geofence.

5.2 Agricultural heavy-lift

Autonomous heavy-lift is a commodity. The DJI Agras T50, from roughly \$19,000 at U.S. retail, carries a 40 kg spray / 50 kg spread payload with RTK positioning and autonomous route-following, available

⁹. Fiber-optic control unspools a thin optical fiber that carries control and video as light, emitting no radio frequency and so immune to RF jamming and detection; maximum distance is capped by spool length (commonly 1–25 km, some designs to ~40–50 km). Diameter and weight figures cited in trade sources are engineering-illustrative, not a universal specification.

¹⁰. Kateryna Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare (CSIS, Mar. 6, 2025) (onboard machine-vision terminal-guidance modules in serial production; Ukraine produced approximately 2 million drones in 2024 and began procuring approximately 10,000 AI-enhanced drones). This paper cites the source only for the fact of fielding and its limited scale; the effectiveness of autonomous guidance is assessed in Paper II, *supra* note 2. Specific named modules are reported in trade press (see Appendix A) and are not independently audited by volume.

¹¹. *Supra* note 2 (the defensive implications of non-emitting control are assessed in Paper II).

through ordinary commercial channels.¹⁴ DJI's roughly 200 kg transport class extends the payload envelope further, though it is a China-market industrial and agricultural lift platform, not a strike system, and is cited only for payload-class maturity.¹⁵

5.3 One-way-attack and loitering munitions

The one-way-attack munition is now a documented, catalogued weapon category with its own market literature. The Shahed-136 class (~200 kg, long range, ~50 kg warhead, GNSS/INS guidance) anchors the high end; its unit economics illustrate the cost collapse — a leaked 2022 export contract priced them at about \$193,000 per unit at quantity (an export price, not a production cost), while independent estimates of domestic production cost have moved from an early \$20,000–\$50,000 band toward roughly \$70,000 by 2025.¹⁶ Simplified and man-portable classes sit below it, and the FPV attack drone — assembled from consumer racing-quadcopter parts — sits at the cheapest end and requires no advanced-state industrial base.¹⁷

6. Cost, Proliferation, and the Incident Record

6.1 Cost curve

An FPV attack drone can be assembled for a few hundred dollars; the quadcopters reportedly used in Ukraine's June 2025 deep strike navigated via an open-source autopilot at as little as about \$2,000 each.

^{13.} Dedrone (Axon) 2025 detection data, drawn from the vendor's Europe–Middle East–Asia sensor network (not a global census): DJI accounted for 83.48% of all drone detections and DIY builds (defined by the vendor as home-assembled drones, including some FPV kits) 9.82% — a 4.3× rise over the Jan.–Aug. 2024 comparison window. Dedrone, *The State of Airspace Defense Today and What's Next* (Sept. 2025) (vendor dataset, 2025 year-to-date). The rising-DIY trend is the salient point. The U.S. baseline is also shifting by regulation: on Dec. 22, 2025 the Federal Communications Commission added all foreign-produced UAS and critical components, including DJI's, to its Covered List, barring new equipment authorizations while leaving previously authorized models in circulation; on Jan. 7, 2026 the Commission 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.

^{12.} Payload capacity has risen from camera-carrying multirotors to 40–50 kg agricultural sprayers to ~200 kg heavy-lift transport drones; machine-vision object recognition and tracking is productized on embedded silicon. Payload capacity is not weaponization; it is cited here only as a maturity indicator.

^{14.} DJI Agras T50 (OEM specifications): from roughly \$19,000 (U.S. retail); ~40 kg spray / ~50 kg spread payload; RTK positioning and autonomous route-following. Cited as an OEM class exemplar of autonomous heavy-lift availability through commercial channels.

^{15.} DJI's ~200 kg heavy-lift class — the FlyCart 200 transport drone and T200 agricultural drone, launched in China in April 2026 — is a China-market industrial and agricultural lift platform, not a strike system; it is cited only for payload-class maturity. Payload capacity does not imply weaponization.

^{16.} Iran Shahed-136 / Russian Geran-2 (OEM/reference specifications): ~200 kg mass; long range (est. 1,000–2,500 km, the top end per U.S. DIA); ~50 kg warhead (larger in some post-2024 variants); GNSS/INS guidance. On cost, two distinct figures must not be conflated: the ~\$193,000 per-unit price is a leaked 2022 Iran–Russia export contract price for a 6,000-unit tranche (leaked documents of the Iranian front company Sahara Thunder, which also show ~\$290,000 per unit at 2,000 units and an initial asking price near \$375,000), not a production cost. Independent production-cost estimates are far lower: \$20,000–\$50,000 (CSIS Missile Threat Project), rising toward ~\$70,000 by 2025 (Defense Express). All are estimates.

^{17.} Class exemplars: the simplified "Gerbera" (est. ~\$10,000; ~300 km in most sources, up to 600 km per Ukrainian defense intelligence); WB Electronics "Warmate" (Poland), man-portable, ~30 km range, ~1.4 kg warhead, unit cost ~\$26,000 as of 2017 (figure is dated). The FPV attack drone, assembled from consumer racing-quadcopter components, sits at the cheapest end of this category and requires no advanced-state industrial base.

¹⁸ Capable commercial multirotors run a few thousand dollars; disposable one-way-attack airframes start near \$10,000. The direction is unambiguous: capable platforms have become cheap.

6.2 Proliferation

The global drone market is large and growing, though estimates diverge sharply by scope and are best treated as directional rather than precise.¹⁹ Production volumes in active conflict are the more concrete evidence, provided they are read as what they are. Ukraine's National Security and Defense Council states installed FPV-drone production capacity above eight million per year across more than 160 firms — a capacity figure, not audited output.²⁰ A Russian manufacturer, cited by the Institute for the Study of War, claims production above 50,000 fiber-optic FPV drones per month — a manufacturer claim, unaudited.²¹ Belligerent planning figures run higher still.²² Read conservatively as capacity and claim rather than audited output, these still establish industrial-scale production of attack drones.

6.3 The open incident record (existence proof)

The record below is grouped by target — political leaders and their residences; infrastructure and military installations; and diffusion to non-state and criminal actors — and is cited strictly as proof that the capability is real and has been used; effects, attribution, and outcomes vary by source and are not adjudicated here.²³

Maduro, Venezuela (2018). Commercially purchased DJI M600 drones carrying explosive charges detonated near the president during a televised address; intent is debated.²⁴ *Proof: commercial drones reached a head of state at a guarded public event.*

Kadhimi, Iraq (2021). Explosive-laden drones struck the Prime Minister's residence inside Baghdad's fortified Green Zone.²⁵ *Proof: a drone reached a hardened, protected compound.*

¹⁸. An FPV attack drone can be assembled for roughly \$400–\$500; Ukraine's June 2025 deep-strike reportedly used quadcopters navigating via the open-source ArduPilot autopilot at as little as ~\$2,000 per drone. Cost figures are open-source estimates.

¹⁹. Global drone-market size estimates diverge sharply by scope and methodology — 2025–2026 figures range from ~\$34 billion (IMARC) to ~\$84–96 billion (Grand View) — and are commercial research-firm projections, not audited data. Treat as directional; no point estimate is relied upon.

²⁰. Ukraine's National Security and Defense Council (Jan. 23, 2026) states installed FPV-drone production capacity above 8 million per year across more than 160 firms; this is stated capacity, not audited output (NSDC, Results of Ukraine's Defense Industry in 2025: FPV Drones, Jan. 23, 2026). Cited as capacity.

²¹. A Russian manufacturer (Ushkuynik director Alexey Chadayev), cited by the Institute for the Study of War via RBC-Ukraine (Sept. 8, 2025), claims production above 50,000 fiber-optic FPV drones per month. A manufacturer/state-adjacent claim; unaudited.

²². Ukraine's commander-in-chief Oleksandr Syrskiy described, in a social-media post of May 8, 2026 (as reported by the Kyiv Post and Ukrainska Pravda), a Russian 2026 plan for 7.3 million FPV drones and 7.8 million warheads for UAVs of various types, attributing the figures to Ukrainian military intelligence. A belligerent planning figure, cited as such.

²³. One further case is noted but not relied upon. Reported drone sightings closed London Gatwick, Britain's second-busiest airport, for ~33 hours over Dec. 19–21, 2018, affecting ~140,000 passengers; no device or culprit was ever conclusively identified. The case is weak as a maturity proof; it shows only that a small drone, or credible reports of one, can paralyze protected airspace.

²⁴. Two DJI M600 drones, each carrying about 1 kg of C-4 per Venezuela's Interior Minister (other official accounts cited three drones), purchased through commercial channels, detonated near Venezuelan President Maduro during a televised address, Aug. 4, 2018; intent and perpetrator remain debated.

²⁵. Explosive-laden drones struck the Iraqi Prime Minister's residence inside Baghdad's fortified Green Zone, Nov. 7, 2021 (three drones; two reportedly shot down); six guards were injured.

Caesarea, Israel (2024). A drone launched from Lebanon struck the Israeli Prime Minister's private residence; the Prime Minister was not present and no one was injured.²⁶ *Proof: a drone reached a head of government's residence in a state fielding one of the most capable integrated air defenses in the world.*

Abqaiq/Khuraib, Saudi Arabia (2019). A combined drone-and-cruise-missile strike temporarily disrupted 5.7 million barrels per day of oil production; attribution is disputed.²⁷ *Proof: the drone component of a strike reached and damaged critical, defended infrastructure.*

Ukraine deep strike (2025). Roughly 117 short-range attack drones, smuggled into Russia and released from concealed truck compartments, were launched against five strategic airbases, striking four; the battle-damage figures are disputed.²⁸ *Proof: clandestine, precise, deep-reach employment at scale has occurred.*

Tennessee, United States (2024–2025). A U.S. person arrested in an FBI undercover operation for planning to attack a Nashville-area electrical substation with an explosive-laden commercial drone pleaded guilty to attempted use of a weapon of mass destruction and attempted destruction of an energy facility.²⁹ *Proof: the lone-actor, domestic, commercial-drone variant has reached the prosecuted-plot stage in the United States.*

ISIS, Iraq and Syria (2015–2017). A non-state group weaponized commercial quadcopters at operational tempo — on the order of 60 to 100 drone attacks per month at the 2017 peak.³⁰ *Proof: a non-state actor fielded weaponized commercial drones at scale.*

26. Hezbollah drone targets Netanyahu's house in Caesarea; PM, wife not home, no injuries, *Times of Israel* (Oct. 19, 2024). Hezbollah subsequently claimed responsibility. Cited only for the fact that a drone reached a head of government's residence.

27. Cong. Rsch. Serv., *Attacks on Saudi Oil Facilities*, IN11173 (2019) (the Sept. 14, 2019 strike on Abqaiq/Khuraib temporarily disrupted 5.7 million barrels/day). The strike was a combined drone-and-cruise-missile attack; attribution is disputed (Houthi claim vs. attribution to Iran). Cited only for the fact that the drone component reached and damaged critical, defended infrastructure.

28. Ukraine's June 1, 2025 deep-strike operation launched roughly 117 short-range attack drones, smuggled into Russia and released from concealed truck compartments, against five strategic airbases (Belaya, Dyagilevo, Ivanovo Severny, Olenya, Ukrainka); the Ukrainka strike reportedly failed, so five were targeted and four effectively struck. Effects are disputed: Ukraine's General Staff claimed 41 aircraft hit (a belligerent claim); a senior NATO official, via Meduza, estimated ~40 damaged, of which 10–13 were fully destroyed (an independent estimate); U.S. officials estimated roughly 20 aircraft hit and about 10 destroyed. The drones were controlled over Russian commercial mobile networks, not by fiber-optic link. Cited here only as proof that clandestine, precise, deep-reach employment at scale has occurred; the defensive significance of the operation is assessed in Paper II, *supra* note 2, which restates the disputed figures without resolving them.

29. Press Release, U.S. Att'y's Off., M.D. Tenn., *Columbia Man Pleads Guilty to Attempting to Use a Weapon of Mass Destruction and Destroy an Energy Facility* (Sept. 9, 2025) (Skyler Philippi; arrested Nov. 2, 2024; plot disrupted before any flight). See also the July 2020 incident near a Pennsylvania electrical substation involving a modified commercial drone, described in a 2021 FBI/DHS bulletin as the first known U.S. case of a drone likely used to target energy infrastructure. See CNN (Nov. 4, 2021) (reporting the bulletin).

30. ISIS weaponized commercial drones (most often DJI Phantom quadcopters) in Iraq and Syria. The threat peaked in spring 2017. See Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (Combating Terrorism Ctr. at West Point, July 2018). The operational-tempo figure ("60 to 100 drone attacks per month" in 2017) and the bundled figures often quoted — at least 56 Iraqi military vehicles destroyed and more than 100 Iraqi soldiers killed or wounded — are from Kyle Brown, Jonathan Askonas & T.S. Allen, *How the Army Out-Innovated the Islamic State's Drones, War on the Rocks* (Dec. 21, 2020), not the CTC report.

Mexican cartels (2021–2025). A coded incident set records 221 cartel drone attacks, of which 136 remain unattributed and 42 (~19%) are linked to the largest identified group.³¹ *Proof: criminal, near-U.S.-border diffusion of weaponized-drone capability.*

7. Consolidated Findings

NO.	FINDING	ANALYST CONFIDENCE
M	Master finding: Small-UAS strike capability is mature, commercially accessible, and already used against critical infrastructure and political leaders — not speculative, and not state-exclusive.	High
F-1	The enabling engineering (commodity autonomy, GPS-independent navigation, fiber-optic control, onboard terminal guidance) is documented and in production, not laboratory-stage.	High
F-2	Strike-relevant capability is available off the shelf or through low-cost assembly; no advanced-state industrial base is required.	High
F-3	Non-emitting control (autonomous and fiber-optic) exists and is produced at scale — a capability fact whose defensive implications are reserved for Paper II.	High
F-4	The one-way-attack / loitering munition is a documented, catalogued weapon category spanning ~\$400 FPV builds to Shahed-class airframes.	High
F-5	Costs have collapsed and production has reached industrial scale in active conflict (read as capacity and manufacturer/belligerent claims, not audited output).	High (direction); figures are capacity/claim
F-6	The open incident record shows weaponized drones reaching critical infrastructure, military installations, and political leaders or their residences on multiple continents, and a lone-actor drone plot prosecuted in the United States.	High (that incidents occurred); effects/attribution vary

Confidence reflects source quality under ICD 203 (supra note 4). Production figures are labeled capacity or claim; incident effects are not adjudicated here.

8. Implications

- **Assess by capability class, not platform.** The enabling technologies are commoditized and diffuse faster than any single model; a platform-by-platform accounting will always lag reality.
- **Treat COTS purchase and low-cost assembly as the baseline threat.** Any planning assumption that a credible small-UAS threat requires a state industrial base is obsolete.

³¹. Austin C. Doctor et al. (NCITE, Feb. 2026) recorded 221 cartel drone attacks 2021–2025 (27 fatal; 77 killed); 136 of the 221 are unattributed, and the Cartel Jalisco Nueva Generación is linked to 42 (~19%), the largest attributed share. Reported fiber-optic command-and-control is an early experiment, treated here as an indicator rather than an established capability.

- **Watch the leading indicators.** Reassess when onboard AI terminal guidance reaches the consumer mass market; when fiber-optic control kits commoditize outside military supply chains; and when conflict-proven autonomy migrates into criminal or terrorist incident records outside active war zones — the documented appearance of a fiber-optic FPV drone in Sinaloa in October 2025 being an early signal.³²

9. Limitations and Scope Conditions

- **Market-size divergence.** Global market estimates differ by an order of magnitude by scope and methodology and are commercial projections, not audited data.³³
- **Production as capacity and claim.** Conflict production figures come substantially from belligerent governments and manufacturers and cannot be independently audited; they are labeled accordingly and read conservatively.
- **Incident record as existence proof only.** Casualty and effect details, attribution, and outcomes vary and several cases are genuinely contested (e.g., Gatwick produced no confirmed device; Abqaiq attribution is disputed; Maduro intent is debated). None of these disputes affects the existence claim.³⁴
- **Effectiveness reserved.** This paper makes no claim about how lethal or how stoppable the weapon is; those questions belong to Paper II.³⁵

10. Conclusion

The evidence is sufficient to retire the “science fiction” objection. The engineering that makes a small drone a precision weapon — autonomy, GPS-independent navigation, jam-resistant control, onboard guidance — is mature and in production; the platforms are cheap and commercially accessible; and weaponized drones have already reached critical infrastructure and political leaders across multiple continents. None of this depends on an advanced-state industrial base, and none of it is speculative. That is the whole of this paper’s claim, and it is deliberately no more than that: whether such a weapon can be stopped is the subject of the second paper in this series, and what it means for U.S. law and leadership protection is the subject of the third. The threat object is real; the series proceeds from there.

^{32.} First documented appearance of a fiber-optic-guided FPV drone in Mexico (Sinaloa, video dated Oct. 3, 2025), Terrogeance, TGA0853 (Oct. 6, 2025); see also supra note 31 (NCITE fiber-optic indicator).

^{33.} Supra note 19 (market-size divergence).

^{34.} On the contested cases, see supra notes 23 (Gatwick), 24 (Maduro intent and drone count), and 27 (Abqaiq attribution).

^{35.} Supra note 2.

Appendix A. Principal Sources

Engineering and navigation

- N. Gyagenda et al., A Review of GNSS-Independent UAV Navigation Techniques, 152 Robotics & Autonomous Sys. 104069 (2022) (peer-reviewed anchor).
- GPS World (2025), Red Cat/Palantir visual-navigation demonstration on a U.S. Army-accepted airframe.
- Named onboard terminal-guidance modules are reported in Ukrainian trade press (illustrative; volumes not independently audited). Cited generically in the main text per source discipline.

Commercial and one-way-attack baseline

- Dedrone (Axon), The State of Airspace Defense Today and What's Next (Sept. 2025) (Europe–Middle East–Asia sensor network; vendor data).
- OEM specifications: DJI Agras T50; DJI FlyCart 200 / T200; Shahed-136/Geran-2; Gerbera; WB Electronics Warmate.

Cost, proliferation, and incidents

- Market projections: IMARC; Grand View Research (directional only).
- Ukraine National Security and Defense Council (2026) (capacity); Inst. for the Study of War, citing Ushkuynik (Chadayev) via RBC-Ukraine (manufacturer claim).
- Don Rassler, The Islamic State and Drones: Supply, Scale, and Future Threats (CTC West Point, July 2018); Cong. Rsch. Serv., Attacks on Saudi Oil Facilities, IN11173 (2019); Austin C. Doctor et al. (NCITE, Feb. 2026); Brown, Askonas & Allen, War on the Rocks (Dec. 21, 2020); DOJ, M.D. Tenn. (Sept. 9, 2025); Times of Israel (Oct. 19, 2024); Terrogeance (Oct. 2025).

Analytic standards

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

Companion papers in this series

- George, C. The Terminal Residual: Warning Time and the Structural Limits of Small-UAS Defense (Paper II, 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, *Not Science Fiction: The Maturation of Small-UAS as a Precision Weapon*, Sanctir Working Paper WP-2026-D1 (2026-10-01), *Drone Threats to Political Leadership: Capability, Defense, and Authority*, Paper I, v1.6.

Keywords: unmanned aircraft systems; drones; loitering munitions; FPV drones; autonomous navigation; fiber-optic drones; technology maturity; proliferation; precision weapons; threat assessment; Russia-Ukraine war; commercial drones.