CONFRONTING UNKNOWNS

A Framework for Anomalous Aerospace Events

June 2026

Confronting Unknowns

A Framework for Anomalous Aerospace Events

Collaboratively authored by members of the
Confronting Unknowns ’26 Program at the
Massachusetts Institute of Technology
and invited colleagues

June 2026

A nation should be capable of saying what it does and does not know about the objects in its own airspace, regardless of whether they turn out to be balloons, classified tests, adversary drones, or phenomena that do not yet have a name. Today it often cannot. *Confronting Unknowns: A Framework for Anomalous Aerospace Events* treats that gap as an institutional problem—of engineering, inference, communication, and coordination—and proposes a four-stage approach for handling anomalous events that resist immediate attribution: Detect, Identify, Respond, and Explain. Three structural forces make the problem urgent: airspace is more crowded than the systems built to watch it, the legislative tempo is accelerating and contradictory, and the online information environment has compressed decision timelines from weeks to hours. We make specific recommendations for Congress, multiple departments and agencies, the intelligence community, research institutions, and the public, drawn from the operational experience of pilots, intelligence analysts, sensor engineers, and communications specialists. Our recommendations are agnostic to what the objects ultimately turn out to be, and opinionated about what we owe each other when we cannot yet say.

Foreword

In early 2026, dozens of engineers, scientists, intelligence analysts, pilots, policy researchers, and communications specialists gathered during a snowstorm at the Massachusetts Institute of Technology to contribute to a new, independent activity on sensemaking and the challenge of confronting anomalous aerospace phenomena. What they produced is in your hands. We offer it to anyone who finds it useful, though we wrote with specific audiences in mind: congressional staff, agency analysts, journalists, scientists, and the concerned citizens trying to make sense of objects that move between sky and sea, seemingly undeterred.

Our program emphatically sidesteps evangelizing speculative or belief-based declarations. Nor are we advocating for any explanation or attribution of unidentified anomalous phenomena. Our argument in this paper is that the United States and its allies must embrace (1) detection architecture, (2) an inference methodology, and (3) communication infrastructure to say what they do and do not know about objects in their own airspace.

Again, the framework does not require taking any position on what anomalous aerospace phenomena are. It requires making the movements of a sensemaker along the spectrum of recognizing, identifying, confronting, and embracing of unknowns as a natural part of being a leader. The future infrastructure for approaching unknowns will be what its participants make of it. We are writing this from inside that participation.

To the enthusiastic cohort who came together for a "no-expense paid trip" during a very Bostonian winter week: the energy you channeled into the Sensemaker Spotlights, the Uncertainty Game, and the Writers' Workshop shapes every page.

I encourage you: Look without flinching, speak without overreaching, and build the institutions that let the truth catch up to the data. Stay signal-sharp!

– Jonathan "JMill" Miller

Lead, Confronting Unknowns Independent Activity
Massachusetts Institute of Technology
Cambridge, Massachusetts

jmill@mit.edu

Authors

This document was collaboratively authored by volunteers among the Confronting Unknowns Independent Activity cohort.

Contributing Authors include Aashka Dave (Postdoc University of Virginia; PhD UNC Chapel Hill), Theodora Skeadas (PhD Cand. King's College London; MPP Harvard University), and Dorothy Wu (PhD Cand. Yale University), and contributors who shall remain anonymous. In addition to direct contribution, the following members also constitute the Editorial Team: Victoria Cheng (PhD UQAM; ALM Harvard University), Davide Lasi (SM MIT), Kevin Romero (MS Johns Hopkins University), Sri Tata (PhD Cand. Yale University), and Susan Winterberg (Venture Consultant; MA Harvard University; fmr. Belfer Center Fellow). The Coordinating Lead and Corresponding Author is Jonathan "JMill" Miller (SM MIT, D.Eng. Cand. Pennsylvania State University).

With gratitude to our pre-publication reviewers: Eric Evans, Jordan Flowers, Ryan Graves, Marik von Rennenkampff, Jessica Souder, and select reviewers who shall remain anonymous, whose corrections and pushback sharpened the paper. All errors that remain are ours.

Expert Acknowledgments

Our guest speakers are the heart of "CU26", the Confronting Unknowns '26 cohort. The invited experts who presented during the January 2026 convening, in alphabetical order by last name: Elena Capuzzo (MIT Security Studies Program; Wargaming Lab program coordinator), Aashka Dave (University of Virginia; information warfare), Phil Erickson (MIT Haystack Observatory; geophysics and atmospheric science), Eric Evans (MIT Lincoln Laboratory; MIT Security Studies Program; sensor management), Jordan Flowers (Disclosure Foundation; sensemaking across markets), Brendan Foster (Americans for Safe Aerospace; UAP morphology and case analysis), Mike Gold (Redwire Space; fmr. NASA administrator for space policy), Francis Govers III (Airbus U.S. Space and Defense; autonomous aerospace systems), Ryan Graves (Executive Director, Americans for Safe Aerospace; fmr. U.S. Navy F/A-18 pilot), Indy Grewal (Shield AI; autonomous systems), Sertac Karaman (MIT Laboratory for Information and Decision Systems; autonomous systems), Greg Knutson (Airbus U.S. Space and Defense; autonomous aerial and maritime systems), Erik Lin-Greenberg (MIT Department of Political Science; co-director, Security Studies Program Wargaming Lab), Tim Lomas (Harvard psychology researcher; UAP assessment framework), Paul Lomax (Yale University; Americans for Safe Aerospace; UAP morphology and case analysis), Scott Ruppel (Department of the Air Force–MIT AI Accelerator), Jessica Souder (fmr. Central Intelligence Agency; intelligence operations), Sri Tata (Yale University; panel moderator), John Thomas (MIT Department of Aeronautics and Astronautics; systems safety and methodology), and Marik von Rennenkampff (contributor at The Hill; case analysis). We strove to interpret and build upon the wealth of insights they shared when preparing this paper.

About the Confronting Unknowns Program

The inaugural convening of the Confronting Unknowns Program at MIT brought together a fifty-plus person cohort for multiple working sessions on the detection, identification, response, and communication of anomalous aerospace events. With no academic credits offered nor any individual's time nor travel compensated, participants came of their own volition. What made the convening unusual and, in our view, possible at all, was the breadth of the institutional participation during its Independent Activities Period and its knack for providing a warm environment for transdisciplinary roll-up-the-sleeves problem-solving.

MIT was deeply present, by design, through leaders, affiliates, and alums of Security Studies Program, Lincoln Laboratory, Haystack Observatory, the Laboratory for Information and Decision Systems, the Department of Aeronautics and Astronautics, the DAF-MIT AI Accelerator, and the Wargaming Lab in the Department of Political Science. Around that MIT core, participants came from Harvard, Yale, the University of Virginia, Carnegie Mellon, Penn State, Johns Hopkins, Brandeis, Redwire Space, Airbus U.S. Space and Defense, Shield AI, Americans for Safe Aerospace, the Disclosure Foundation, The Hill, the Intelligence Community, and the wider community of operators, researchers, and communicators who have worked this problem in public and behind closed doors.

About The End Effector

The Confronting Unknowns Program was formulated under the auspices of The End Effector, the independent practice led by Jonathan "JMill" Miller. Confronting Unknowns at MIT is led on a volunteer basis; our convening logistics, editorial work, branding, and media production are underwritten by The End Effector. Visit endeff.com for more about that public-benefit educational endeavor.

Disclosures and Editorial Independence

This report is an educational and research product of the Confronting Unknowns program at MIT. It is expressly not to be interpreted as an MIT-affiliated official statement, but rather as a personal opinion of the authors. References to companies, technologies, and investors are illustrative and based on publicly available information and contributor expertise. Inclusion does not constitute endorsement by MIT, the Confronting Unknowns program, The End Effector, or any contributor's affiliated institution or organization, and omissions should not be interpreted as negative judgments.

Editorial decisions were made in service of the report's educational and analytical goals. The report should not be read as investment, procurement, legal, or policy advice. MIT-affiliated contributors remain subject to applicable MIT policies on conflicts of interest and commitment.

How to read this paper

We recommend that all readers prioritize the *Executive Summary*, *Part I: The Problem*, and the closing sections of *Part IV: An Action Agenda for New Unknowns* (i.e. *"The Most Important Change to Make..."* and *"An Argument That Does Not Depend on the Answer").* From there, pick the path that fits your work.

Essentials Path

For Congressional staff, journalists, and policy generalists, read:

1. *"The Confronting Unknowns Framework"* (Part I),
2. *"Learning from Today: New Jersey Media Melee"* (Part III), and
3. *"Implications by Audience: Action"* (Part IV).

Operator Path

For emergency managers, agency leads, and congressional-oversight staff, read:

1. *"Crisis Playbook"* (Part I),
2. *"Diagnostic Markers for the Next Incident"* (Part III), and
3. *"Action 3: Improve Aerospace Incident Readiness & Response"* (Part IV).

Researcher Path

For researchers, sensor specialists, and data practitioners, read:

1. *Part II: Detect & Identify,*
2. *Appendix D: Sensor Capabilities – Observables, Modalities, and Limitations*, and
3. *Appendix H: Simple Probabilistic Case Analysis.*

Table of Contents

Figure Index

Table Index

Inset Index

Executive Summary

The case for confronting anomalous aerospace events does not depend on what they turn out to be. Whether the objects are ordinary or extraordinary, the institutional work required to face them is the same, and it is overdue. A nation should be able to say what it does and does not know about the objects in its own airspace. Today it often cannot, as evidenced by large-scale incidents over a wide-range public, critical, and military with real consequences. The gap is largely about engineering, inference, communication, and the systems that connect them – not just about the objects themselves. A nation that cannot identify what is in its airspace has a safety problem, one that cannot communicate honestly about what it does and does not know has a trust problem.

Three forces make this urgent now. Airspace is more crowded than the systems built to watch it: more than one million drones were registered with the Federal Aviation Administration (FAA) by December 2024, tracked by systems designed for an earlier era. The legislative response is accelerating and contradictory, with states standing up Unidentified Anomalous Phenomena (UAP) research centers and airspace task forces while Congress weighs dissolving a federal office meant to coordinate the problem. And the online information environment has compressed decision timelines from weeks to hours: the New Jersey drone incursions generated more public discourse in 72 hours than the entire Project Blue Book archive, leaving officials to choose between speaking early and ceding the narrative to speculation.

New Jersey showed the cost. Over the 76 days between the first sighting at Picatinny Arsenal and a White House statement that the drones had been "authorized... for research and various other reasons," no entity or authority held the seam between the FAA, Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Department of Defense (DoD), and state emergency management. A year later, the governor's office still had no definitive explanation. The most consequential signals were never the objects; they were the institutional responses of contradictions, silences, expertise refused, closure declared without explanation.

We propose treating anomalous events as a pipeline of four interdependent stages. 'Detect' captures and preserves evidence with sensors and observers calibrated for objects outside known profiles. 'Identify' translates that evidence into ranked hypotheses under explicit uncertainty, rather than a binary "resolved / unresolved" verdict. 'Respond' coordinates the inter-agency decision chain so that "who decides, and on what evidence?" has an answer before the next event. 'Explain' communicates findings and uncertainty to the audiences who need them—commanders, congressional staff, journalists, and the public.

Part I: The Problem explains the problem being faced. *Part II: Detect & Identify* and *Part III: Respond & Explain* develop approaches to a solution in full. See *Part IV: An Action Agenda for New Unknowns* for detailed policy prescriptions.

Our recommendations are agnostic to what such anomalous objects turn out to be. Four are the most impactful:

1. Stand up an inter-agency communication protocol for anomalous aerospace incursions. Direct the National Security Council (NSC), FEMA, and other federal agencies to develop and exercise it, on the model of existing pandemic, nuclear-incident, and natural-disaster playbooks. This is the one recommendation the others depend on: every sensor upgrade and analytic method still has to run through the same inter-agency seam that failed over New Jersey.

2. Create named research funding categories for anomalous-phenomena studies at NSF, DOE, and NASA. The absence of a category under its own name is what makes the field institutionally invisible today; naming it is a simple and impactful way to facilitate serious academic and institutional participation.

3. Train the communicators who will face the next event—public affairs officers, journalists, platform trust-and-safety teams, and frontline operators and clinicians. Map the information environment, build a citable clearinghouse of vetted sources, and engage the public deliberately.

4. Pursue a Church Committee–style formal accounting of prior information-management practices. Before any new response infrastructure is built for aerospace events, we must understand the gaps of recent and past systems. Any communication or disclosure framework will be weighed down by an unresolved historical ledger. Whistleblower protections pair with this recommendation.

This is the throughline stated at the outset: the argument does not depend on the answer. If the unknowns prove mundane, the same infrastructure improves aerospace safety, operational awareness, and public trust. If they, or even one, prove extraordinary, it provides the evidentiary foundation without which extraordinary claims cannot be responsibly evaluated. The first step does not change. What it requires is better engineering, better inference, better communication, and better institutional design.

Part I: The Problem

Recurring Incidents, Repeating Failures

1. Why is this moment more urgent than earlier waves of unidentified-object sightings?
2. What happened over New Jersey in late 2024 and why has no one explained it since?
3. Is New Jersey an isolated episode, or one instance of a recurring pattern that keeps ending the same way?
4. What would it take to respond to such events without first resolving what the objects are?

Reports of unidentified objects over military and civilian airspace go back decades, and so do the institutional struggles to explain them. What separates the present moment is not the objects but the conditions surrounding them. Three forces have converged that did not previously exist together: a crowded airspace, a contradictory legislative response, and a compressed information environment. None of the three depends on what the objects turn out to be. Together they leave less margin for getting the next response wrong.

Why Now Is Different

The airspace is getting more crowded. Commercial and military drones, autonomous systems, and low-Earth-orbit satellite constellations mean more objects in the sky than existing systems were designed to track. More than one million drones were lawfully registered with the Federal Aviation Administration (FAA) by December 2024 [1]. The U.S. Army alone requested more than $400 million for counter-small-unmanned aircraft systems (UAS) systems in fiscal year 2025 [2]. The volume of potential anomalous events will increase whether the underlying phenomena are changing.

The legislative tempo of UAP-oriented legislation is accelerating, yet its direction is increasingly contradictory. The proposed Unidentified Anomalous Phenomena Disclosure Act (UAPDA) [3] would establish formal declassification processes and an independent review board with eminent-domain authority over recovered materials. The Safe Airspace for Americans Act addresses operational response authorities. New Jersey passed Assembly Bill A-5712 in January 2026, establishing a state-funded Center for the Study of Unidentified Aerial Phenomena with $2.5 million in research grants. Vermont introduced Act H.654, proposing a state airspace safety task force and House Bill 5422 is advancing in Connecticut, proposing a similar task force structure. There are legislative infrastructures being built in the absence of adequate federal action. Meanwhile, at the federal level, House Bill H.R. 8197 would dissolve the All-domain Anomaly Resolution Office (AARO) entirely and prohibit creation of any future centralized UAP office, redistributing its functions across the Pentagon. State legislatures are building new capacity while Congress is considering dismantling it federally. The contradictory trajectories make the coordination problem worse with each session.

The online information environment has compressed decision timelines and is driving conflicting public narratives. A sighting that in 1997 took weeks to reach national awareness and months to necessitate an offi-

cial response (the Phoenix Lights [4]) now saturates social media within hours. The 2024 New Jersey drone incursions generated a volume of public discourse within seventy-two hours that dwarfs the entire Project Blue Book [5] case archive in scale. Decision-makers who once had weeks of quiet investigation before issuing public statements now face a choice between immediate communication and ceding the narrative to speculation. The media and entertainment industry compounds this: the *Age of Disclosure* documentary [6], featuring 34 senior government officials, reached mainstream audiences in 2025. The information environment will not slow down to wait for institutional readiness.

As said by Ryan Graves, a former Navy F/A-18F pilot who testified before Congress regarding his squadron's UAP encounters in 2023 and now leads Americans for Safe Aerospace, "There is really no closed system that would actually allow us to respond in a manner that would prevent an adversary from causing harm." Radar operators, pilots, intelligence analysts, and public affairs officers are, in most cases, doing their jobs competently within the systems they have been given; the unresolved volatility lies in the loose patchwork connecting those systems and, and in the absence of mechanisms for them to align.

These pressures expose three failures that recur across incidents worldwide, including over restricted military airspace: our ability to detect, identify, and track unknown objects is inadequate; we lack the institutional capacity to communicate and coordinate across agencies; and we lack clarity over who holds the authority to respond. Left unaddressed, the same gaps that produce confusion today could fail to surface a genuine homeland-security threat tomorrow. The New Jersey events of late 2024 made all three visible at once.

> *...our ability to detect, identify, and track unknown objects is inadequate; we lack the institutional capacity to communicate and coordinate across agencies; and we lack clarity over who holds the authority to respond.*

Something above New Jersey

The Picatinny Window

On the evening of November 13, 2024, personnel at Picatinny Arsenal in northern New Jersey observed lights of unknown origin maneuvering above the installation [7]. Within days, reports multiplied across New Jersey and into neighboring states. The FAA issued temporary flight restrictions. A state senator called for a limited state of emergency. The FBI and DHS issued a joint statement asserting "no evidence" of a threat. President-elect Trump posted on Truth Social, "shoot them down." President Biden said, "nothing nefarious, apparently." By December 18, the FAA had imposed 22 flight restrictions across the region. Communities organized watches, launched drones, shone lasers at the sky, and fired weapons. A retired Army counter-UAS specialist offered his expertise to law enforcement and was frozen out. Twenty-one mayors signed a letter to the governor demanding answers. A classified briefing for 185 mayors produced no answers. The incident did not resolve; it remains unaddressed [8].

On January 28, 2025, Press Secretary Karoline Leavitt stated: "After research and study, the drones that were flying over New Jersey in large numbers were authorized to be flown by the FAA for research and various other reasons." Yet even an entire year later, the governor's office confirmed it had never received a definitive explanation from federal authorities [8]. Figure 1 traces a 76-day arc from the first Picatinny sighting on November 13, 2024, to the White House closure on January 28, 2025.

The most consequential signals were never the objects in the sky. They were the institutional responses: contradictions, silences, expertise refused, closure declared without explanation. Each response shaped the next, and by the end those responses had produced consequences far more durable than the objects ever did: state legislation, congressional hearings, and proposals to restructure how the federal government handles the problem.

Figure 1: Timeline of the New Jersey drone incursions, November 2024 – January 2025.

A Pattern of Incidents Worldwide

The New Jersey airspace incursions were among the most publicly visible instances of a recurring pattern of events. New Jersey did not begin that pattern, but it brought the pattern into sustained public view; comparable episodes preceded it and have continued since, across military installations and civilian infrastructure in both North America and Europe. What links these events is less any single explanation for the objects themselves than the response sequence each one set in motion. (See *Appendix G: "Drone Wave" Timelines* for a comprehensive timeline of recent 'drone incursions' or 'waves.')

- **North American Aerospace Defense Command (NORAD) Shootdowns after Chinese Balloon Incident:** In February 2023, the military shot down three objects over North American airspace; those three were declared likely benign, but despite a major mobilization little further explanation ever followed. They came amid heightened sensitivity after NORAD tracked a Chinese surveillance balloon from Alaska to South Carolina, drawing days of national attention before an F-22 shot it down off Myrtle Beach.
- **Langley Air Force Base:** In December 2023, unidentified aerial objects conducted sustained incursions over Langley Air Force Base in Virginia, home to the Air Force's first fighter wing, over roughly 17 days. The objects operated at night, exhibited flight characteristics inconsistent with standard commercial or recreational drones, and evaded identification despite the base hosting some of the most advanced aerospace sensor systems in the DoD inventory. The Wall Street Journal reported that the incidents prompted the temporary relocation of F-22 Raptors to Naval Air Station Oceana which affected air coverage of the U.S. Capitol [9]. No public attribution has been made.
- **Denmark Drone Wave:** In Europe starting around September 2025, a wave of unknown objects analogous to the "NJ wave" was seen across NATO member-states' military bases and civilian infrastructure in Europe [10], prompting shutdowns and precautionary measures and disruptions even at public airports. These public safety issues mixed with geopolitical ones in the backdrop of the war in Ukraine, leading to suspicion and presumption of Russian involvement despite no evidence being presented on either side.
- **Barksdale Air Force Base:** In early March 2026 unknown objects were reported over Barksdale Air Force Base in Louisiana, a nuclear-capable bomber base. This prompted a response from the Air Force Global Strike Command [11] although as of this writing no official explanation has been provided. This is despite an internal Air Force briefing document, quoted by ABC News, warning that "drone incursions at BAFB pose a significant threat to public safety and national security" because they require flightline shutdowns and place manned aircraft already in flight at risk [12].

The same structure repeats across these incidents:

1. an object appears,
2. existing systems fail to identify it,
3. institutional communication fractures, and
4. the public is left with contradictory narratives and residual distrust.

.

Figure 2 below shows the geographic and temporal clustering of major incidents across U.S. military and critical-infrastructure sites, focusing on late-2024 incidents.[1] Figure 3, further below, shows additional late-2024 incursions over U.S. sites in Europe, as well the European wave of 2025 over many nations' critical civilian and military infrastructure.

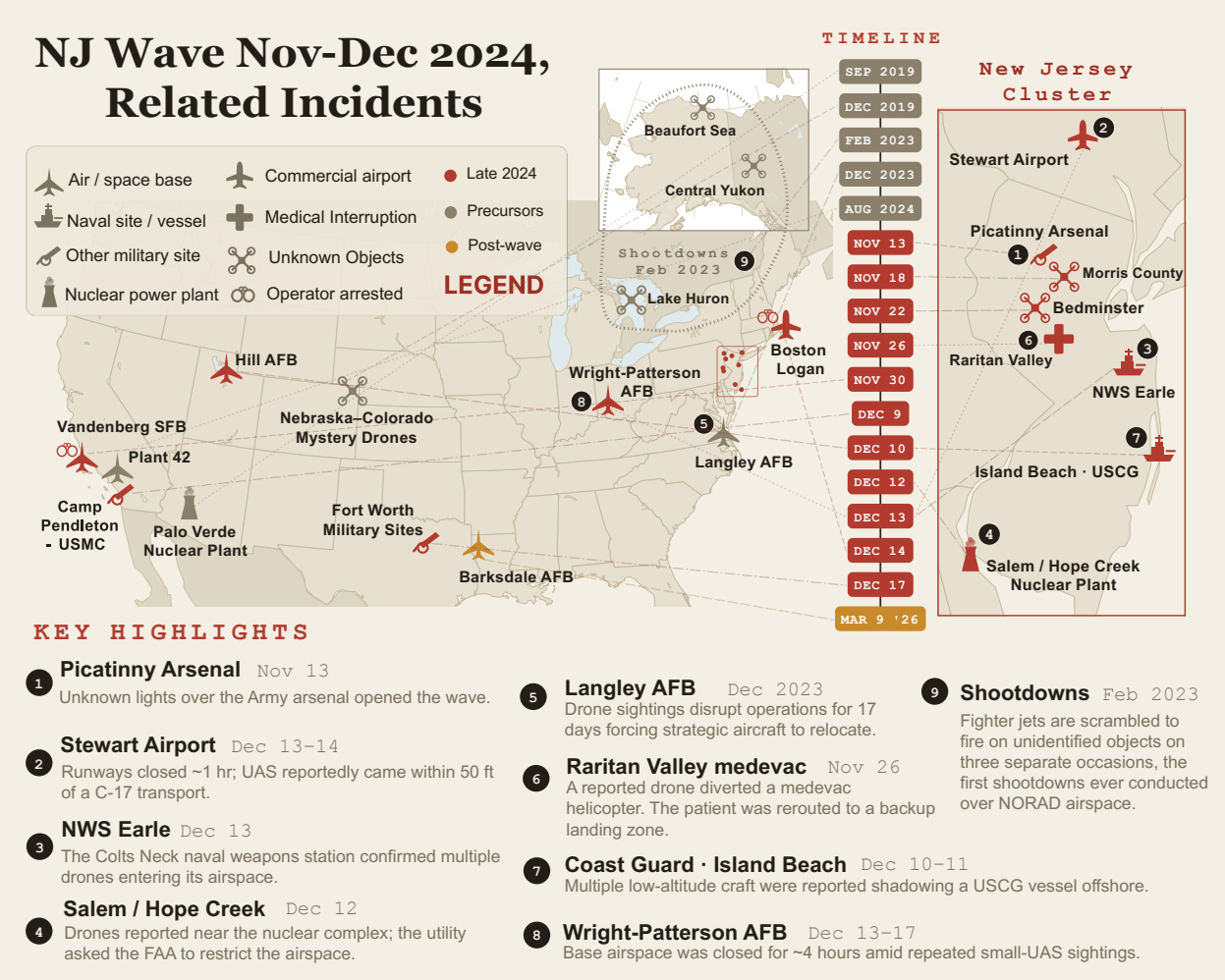

Figure 2: Timeline of major incursions between 2019–2024 of unknown objects or drones over the U.S. involving critical infrastructure or significant response by military or law enforcement, with particular attention on the late-2024 wave concentrated over New Jersey.

[1] We are focusing on higher-profile events that have been publicly reported. Ongoing public records investigations indicate a number of events over critical infrastructure of analogous severity to the ones we list, except without comparable media coverage. See [13], for example—we thank its author, John Malaska, for sharing a number of valuable details, many of which will be available in his forthcoming articles.

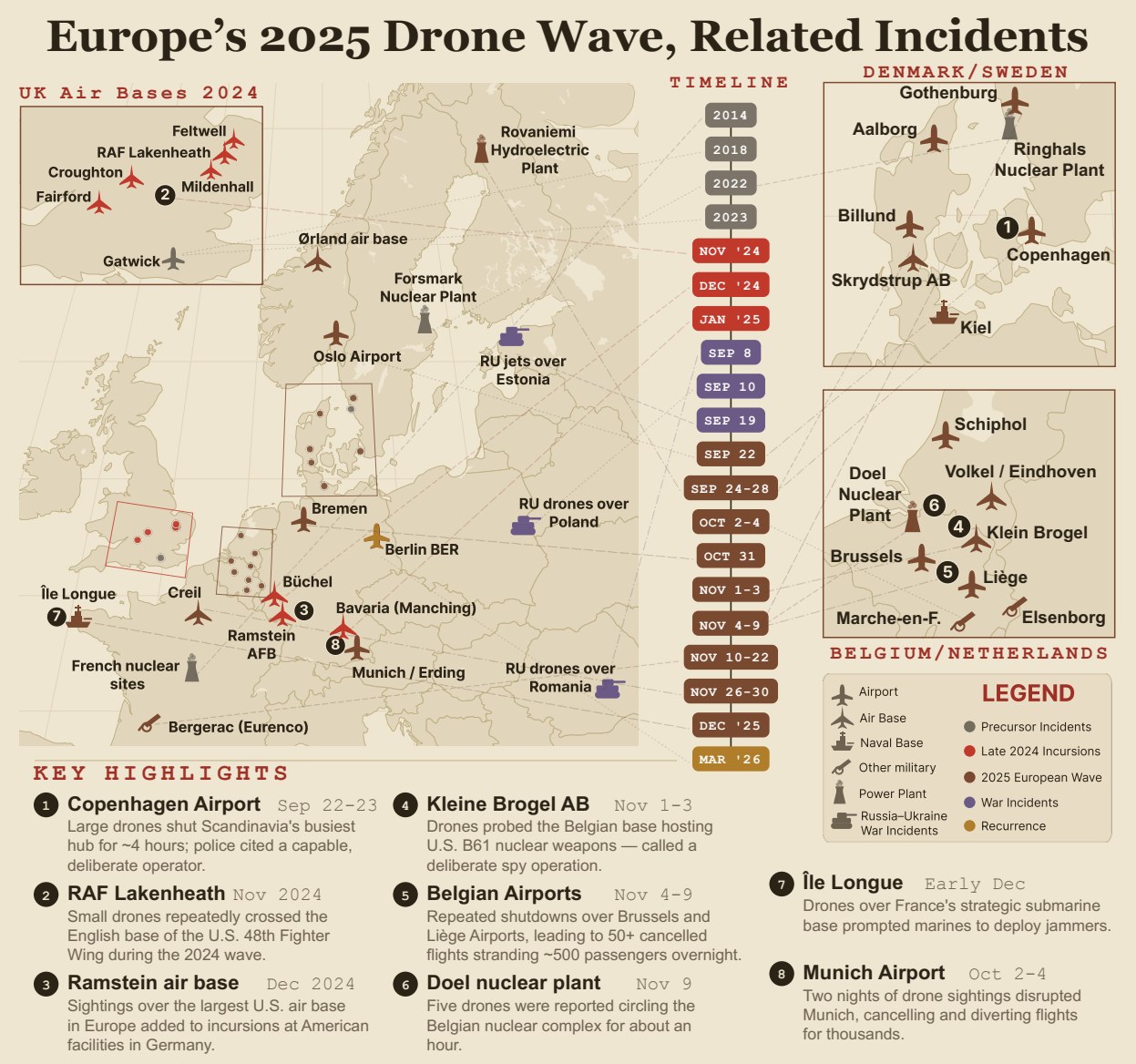

Figure 3: Timeline of the recent European Wave of major aerial incursions, mostly reported as 'drones', over military and civilian critical infrastructure across Europe, with particular attention paid to the late-2025 wave, and incidents in late-2024 coincident with the so-called NJ Wave.

The Confronting Unknowns Framework

The Confronting Unknowns Framework (CUF) proposes treating anomalous events as a pipeline of four interdependent stages:

Detect, Identify, Respond, and Explain (D-I-R-E).

It differs from legacy approaches in that uncertainty, rather than being forced to dissolve into a resolved/unresolved dichotomy, is made explicit and carried all the way from detecting to explaining anomalies to the audiences who need them: operational commanders, congressional staff, journalists, as well as the wider public who watch the same skies. As shown in Figure 4 below, data flows left-to-right through Detect → Identify → Respond → Explain. At each junction, the downstream stage targets uncertainty in the previous stage to offer iterative improvement, whether by increasing the sophistication of the analysis or offering more concrete actions and outcomes, or both.

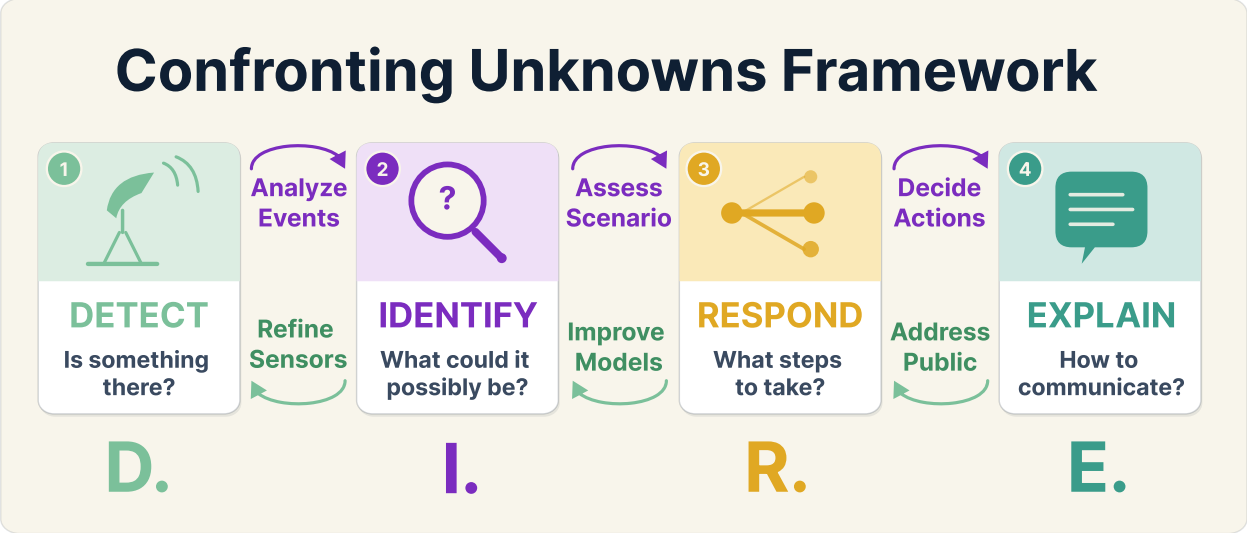

Figure 4: The Confronting Unknowns Framework, in which data flows through Detect, Identify, Respond, and Explain stages.

Our perspective is that central to thoughtful emergency responses is the ability to retain a sense of proportion for what could be causing an event, without jumping to conclusions.[2]

[2] Supporting CUF is a set of hypotheses and a suggested approach to managing it. See *"Identifying Unknowns"* in *Part II: Detect & Identify*.

Detect: Is Something There?

Military radars are optimized for known profiles: aircraft with expected signatures, speeds, and altitudes. Air traffic control tracks cooperative targets broadcasting transponder signals. Weather radars, satellite constellations, and maritime monitoring systems observe the relevant domains but were never designed to correlate their data around anomalous events. Indeed, most of the sensor stack inherited the mission of an earlier era. Post-Sputnik radars were tuned to detect intercontinental ballistic missiles.

None of these systems was tasked to characterize objects whose kinematics—the geometry of motion—did not match the threat the system was built to detect. That's why we have the paradox of capable sensors but face siloed data, processing pipelines tuned to suppress the signals that matter here, and retention policies that discard potentially relevant information before anyone thinks to look for it.

> *Capable sensors, siloed data, and processing pipelines are tuned to suppress the signals that matter here, and retention policies discard relevant information before anyone thinks to look for it.*

Identify: What Is It?

The conventional UAP approach sorts anomalous events into "resolved" and "unresolved." This is useful for topline bookkeeping but poorly suited to events that develop over time, involve partial evidence from multiple modalities, or demand decisions before definitive attribution. A radar track that is 60% consistent with a commercial drone, 25% consistent with an atmospheric artifact, and 15% consistent with something genuinely unusual is poorly summarized by the "unresolved" label.

Respond: What To Do, and Who Decides?

Respond is the stage where identification becomes action: who is notified, who decides, on what evidence, and with what authority. The New Jersey incursions showed what happens when none of that is settled in advance. No agency held the seam between the FAA, DHS, FBI, DoD, and state emergency management, because the event never crossed any single agency's threshold for a credible threat, and so the response was improvised in public.

This paper treats response in three places rather than one. The *"Crisis Playbook"* later in this Part gives senior decision-makers a structured way to act in the first hours of an incident: classify the situation, work a pre-designated contact chain, guard against decision traps, and select a proportionate, authorized response. *Part III: Respond & Explain* examines how the New Jersey response broke down and what an aligned response would have looked like.

Part IV: An Action Agenda for New Unknowns translates both into an action agenda for readiness and inter-agency coordination.

Explain: What To Say, By Whom and When?

When communication is treated as an afterthought it becomes the most consequential signal of all. The information vacuum[3] in 2024 was filled by a Congressman's claim of an Iranian mothership, a loose-nuke theory that migrated from a podcast to mainstream media, and a mass-hysteria narrative that dismissed credible eyewitnesses alongside dubious ones. The framework provides a fourth option with Explain: follow a structured protocol that preserves evidence, manages uncertainty, and communicates clearly under uncertainty.

The following tables summarize strategies for four audiences. Policymakers should review Table 1 below, Operators refer to Table 2, Researchers to Table 3, and Communicators to Table 4.

> *A radar track that reads as 60% consistent with a commercial drone, 25% consistent with an atmospheric artifact, and 15% consistent with something genuinely anomalous cannot simply be labeled 'unresolved'.*

[3] The measurement of information vacuums is ongoing and includes work among some of the authors [14].

Table 1: Strategy for Policymakers.

For Policymakers	
The New Jersey incursions were not a failure because anyone refused to act; they were a failure because no one owned the boundary between FAA, DHS, FBI, DoD, and state emergency management. The single highest-leverage federal action is to designate an inter-agency communication protocol for anomalous aerospace incursions, analogous to the playbooks that already exist for pandemics, nuclear incidents, and natural disasters. State-level capacity-building (A5712, H.654, HB 5422) is constructive but will fragment the problem further without a federal-state coordination layer. Various pending bills cut in opposite directions: the UAP Disclosure Act would build institutional capacity, while HR 8197 would dissolve AARO. The unmanaged contradiction between UAPDA and HR 8197 is the federal-level analogue of the December 2024 boundary problem.	
Actions	**Impact**
1. Fund named research tracks at NSF/DOE/NASA. 2. Direct NSC and FEMA to establish crisis protocols. 3. Initiate a "Church Committee"-style historical ledger accounting.	Validates academic participation, fosters emergency readiness, and builds public trust.

Table 2: Strategy for Operators

For Operators	
Pilots, controllers, radar techs, and counter-UAS teams are, in most cases, doing their jobs competently inside systems that were never built to talk to each other. Preservation of the raw record (calibration state, ancillary telemetry, chain of custody) before triage is incredibly useful.[4] First responders and frontline operators should expect, and prepare to answer honestly, questions such as, “How do you know it's not a danger if you don't know what it is?”	
Actions	**Impact**
1. Enforce raw sensor data and metadata preservation before triage or transfer. 2. Explicitly log multi-sensor confirmations, recognizing that the correlated product may classify differently than any single input. 3. Utilize a spectrum of explanatory hypotheses, so handoffs carry calibrated uncertainty rather than premature label. 4. Generate a releasable tear-line summary for cross-agency handoffs.	Eliminates data loss, prevents premature closure, and builds an auditable operational picture.

[4] Once an event has been reduced to a narrative summary, the sensor metadata needed to re-analyze it is usually gone. NASA's independent study team found that UAP analysis is hampered by poor sensor calibration, missing sensor metadata, and a lack of baseline data, and AARO itself reports that hundreds of its cases lack sufficient data to support analysis, with case resolution constrained by a shortage of timely, actionable sensor data.

Table 3: Strategy for Researchers

For Researchers	
The empirical record visible from outside government is fragmentary: the New York Times videos in 2017, congressional testimony, thousands of narrative reports from contemporary and historical organizations like Americans for Safe Aerospace (ASA), National Aviation Reporting Center on Anomalous Phenomena (NARCAP), Mutual UFO Network (MUFON), etc., and the open-source residue of incidents like Langley and Barksdale. No civilian science agency offers a competitive grant category under which UAP-relevant work can be submitted by its actual name. The result is a research community that exists but is institutionally invisible. There are falsifiable studies that could materially affect our understanding without requiring declassification such as re-analysis of weather radar archives during known incursions or developing atmospheric-optics models for the most common misidentification modes.	
Actions	**Impact**
1. Execute observational feasibility studies. 2. Build pipeline-first artificial intelligence (AI) models using commercial foundations. 3. Focus on cross-disciplinary Focused Research Organization (FRO) structures.	Maximizes data collection efficiency and delivers falsifiable, peer-reviewed data.

Table 4: Strategy for Communicators.

For Communicators	
The most useful intervention is also the least dramatic: maintain the distinction between the phenomena and the institutional response, because conflating them is precisely what produces both premature debunking and conspiratorial drift. Journalists, response communicators, and the public inherited a fragmented information environment: a State Senator calls for a limited state of emergency and a Congressman invokes an Iranian mothership in the same week[15]—"what is in the sky" and "what is happening in government" became indistinguishable in the news feed.	
Actions	**Impact**
1. Implement the Observer Education Feedback Loop. 2. Pre-draft intermediate "unknown" response templates. 3. Train public affairs officers and platforms.	Minimizes speculation, manages disinformation, and raises incoming reporting signals.

Crisis Playbook

This section sets out an emergency protocol for senior decision-makers confronting airborne anomalies over military installations. It provides a structured framework for action during the first hours of an event, when the identity, intent, and significance of the object remain uncertain and the situation is still evolving.

Drawing on crisis-management practices from defense, public health, and critical infrastructure, the playbook replaces the legacy defaults of "ignore," "classify," or "call a press conference" with a deliberate response sequence built around four capabilities:

1. **Proper Situation Classification:** A taxonomy of event types (from routine airspace anomalies to multi-domain events) to determine the response posture within minutes.
2. **Streamlined Contact Protocols:** A clear inter-agency hierarchy among the Federal Aviation Administration (FAA), Department of Homeland Security (DHS), Department of Defense (DoD), All-domain Anomaly Resolution Office (AARO), state emergency management, scientific advisors, and media communication chains.
3. **Decision-Trap Awareness:** Structural workflow checks to counteract cognitive vulnerabilities like premature closure ("it's just drones"), authority bias, availability bias, and anchoring.
4. **Appropriate and Graduated Response Options:** A tiered menu of proportionate actions, spanning enhanced passive monitoring to physical intercept, backed by pre-identified legal authorities and escalation criteria.

The institutional investments that make these response options possible, including sensors, protocols, research funding, and public-trust infrastructure, are the subject of *Part IV: An Action Agenda for New Unknowns*.

1. Classify the Situation

The first task is to set a response posture within minutes, before anyone can say what the object is. Classification is therefore keyed to what can be observed immediately, where the object is, how it is behaving, and how long it persists, rather than to a resolved identity. A workable scheme runs in four tiers as seen in Table 5 below.

Table 5: Situation classifications to set a response posture before identity is known.

Tier	Trigger	Response posture
Tier 0: Routine	Identified or low-concern traffic in ordinary airspace	Log and monitor; no activation
Tier 1: Ambiguous	Unidentified object, no threat indicators	Activate detection and identification; designate an incident commander; prepare public communication before speculation fills the gap
Tier 2: Concerning	Unidentified object with risk factors: restricted-airspace penetration, proximity to critical infrastructure, coordinated movement, or persistence across hours	Interagency activation; graduated-response options on the table
Tier 3: Hostile or multi-domain	Confirmed hostile act, or an event spanning air, cyber, and ground at once	Full incident command under defensive authorities

Posture rises or falls as evidence accumulates. What matters is that the event enters a defined tier at once, rather than waiting on an identification that may never arrive.

2. Work the Contact Chain

Even as an event may fail to cross any single agency's[5] threshold for a credible threat, a seam of inter-agency communications, decision-making, and authority-handover must be held, with means for escalation depending on severity. Having a contact chain in advance can settle uncertainty over who and how to hold the liminal area between agencies. Three elements should be fixed before an event rather than during one:

- A designated Incident Commander for each tier and location, so that "who is in charge?" has an answer at minute one.
- A notification order naming which agencies are called, in what sequence, and with what authority: the FAA and the air-defense element (NORAD) first, then DHS, FBI, AARO[6], and state emergency management, with scientific advisors and a public-affairs lead brought in as the tier warrants.
- A single Joint Information Center authorized to speak, so that one account reaches the public rather than competing statements that can drive mis-information cascades. A classified-to-unclassified bridge

[5] Such as but not limited to FAA, DHS, FBI, DoD, and state emergency management.

[6] Or a contemporaneous, authoritative anomaly-focused organization.

should run alongside it, so the people who need to act are not blocked by the classification of what is known.

3. Guard Against Decision Traps

Ambiguity under time pressure is the exact condition in which judgment degrades, and the usual failure is a premature collapse of uncertainty in one direction or the other.[7] Most common traps can be countered with modest preparations and protocols:

- **Premature closure:** the urge to call an event "resolved" simply to end the discomfort of not knowing
  Counter*:* require an explicit set of ranked hypotheses (the H1-H5 hypothesis space), and treat "unresolved" as an honest, reportable state rather than a failure.
- **Anchoring:** the first explanation offered tends to dominate everything after it.
  Counter: generate competing explanations before settling on any one.
- **Authority bias:** deferring to the most senior voice instead of the evidence.
  Counter: keep the assessment of evidence separate from the rank of the person making it.
- **Availability bias:** over-weighting the most recent or most vivid event.
  Counter: reason from current landscape, not from the last drone wave.

4. Match the Response to the Threat

Response should rise and fall with the situation tier, and each step should be authorized in advance rather than improvised.[8] The institutional version is deliberate and proportionate. A graduated ladder runs roughly as shown in Table 6 below.

[7] In the December 2024, a "no threat" reassurance and an "Iranian mothership" rumor were the same error pointed opposite ways.

[8] *Part III: Respond & Explain* documents what happens when escalation is left to improvisation at the community level: observation gives way to interception, and then to undesired effects such as civilians lasing commercial aircraft.

Table 6: Graduated Response Ladder showing proportionate actions that can be pre-authorized.

Rung	Action	Authority to authorize	Move up a rung when...
1. Passive monitoring	Enhanced sensor attention; no engagement	Local or agency operational lead	The object persists or moves toward a higher-concern area
2. Active tracking and identification	Cue additional sensors, dedicate assets, work the identification pipeline	Agency operational lead, with inter-agency notification	Risk factors appear: restricted airspace, infrastructure proximity, coordinated movement
3. Deterrence and airspace control	Position assets, issue a Temporary Flight Restriction where warranted, signal presence	Designated Incident Commander; FAA for airspace measures	Threat indicators strengthen or non-cooperative behavior continues
4. Physical interdiction	Defeat or neutralize the object	Confirmed engagement authority over the homeland (legally unsettled)	A hostile act is confirmed or a threat is imminent

Two requirements make the ladder safe to use. Every rung needs a named authority settled before the event, because the unresolved question of who may authorize engagement over the homeland is exactly the gap that produces either hesitation or overreaction in the moment. And the ladder needs explicit de-escalation criteria, not only escalation criteria, so a posture can stand down as cleanly as it was raised. Skipping rungs under pressure is the failure mode, so the menu exists to prevent it.

Taken together, these four moves are the acute-phase complement to *The Confronting Unknowns Framework*: the framework is how to make sense of an event, and the playbook is how to hold a response together while that sensemaking is still underway.

Part II: Detect & Identify

The Science Behind the Confronting Unknowns Framework

1. Why do modern sensor systems fail to reliably detect events that fall outside the categories they were built for?
2. How do we tell a genuine anomaly from a sensor failure or a processing artefact?
3. What does it mean to identify an event probabilistically, rather than as resolved or unresolved?
4. What can artificial intelligence add to this work, and what should it not be asked to do?
5. How does an analyst move from raw sensor data to a ranked list of explanatory hypotheses?

The Confronting Unknowns Framework (CUF) requires all its constituent elements of Detect, Identify, Respond, and Explain to perform effectively and their handoffs to carry an event from first observation through to public communication. Here we cover the key challenges of the Detection and Identification elements of CUF, including discussing gaps and opportunities for improvement in the current practice of dealing with anomalous events, and some of the limitations of our own framework and direction for future research.

Detecting Unknowns

Detecting unknowns starts with observing possible anomalies through technological sensors, human sensory observation (visual sighting), or both. A credibility dilemma has plagued observations of anomalies such as UAP. Keep or discard observations that go against commonly perceived beliefs of what is possible or real? We dive deep into the gaps and opportunities of human observations and sensors in this section.

What Makes Something Anomalous: Six Observables

The Confronting Unknowns Framework endorses the Unidentified Anomalous Phenomena (UAP) definition from U.S. policy discussions, including the UAP Disclosure Act, as events exhibiting one or more of six observables:

- Instantaneous acceleration absent apparent inertia
- Hypersonic velocity absent a thermal signature and sonic shockwave
- Transmedium travel (e.g., space-to-ground, air-to-undersea)
- Positive lift contrary to known aerodynamic principles
- Multispectral signature control demonstrating intelligent stealth capabilities
- Physical or invasive biological effects on close observers or the environment

We discuss examples based on "Aerial" UAP, which is perhaps the most common type of anomalous incidents, while recognizing that "A" stands for "Anomalous," a broader category that spans across multiple domains (space, submerged, transmedium, etc.).

Inset A: Observables associated with Unidentified Anomalous Phenomena.

The Observation Credibility Dilemma

A core challenge of UAP detection has been evaluating the credibility of any given observation. The high volume of observations that have been outright dismissed due to "low credibility" of either the technological sensor or the human observer has hindered operational decision making and slowed sensemaking. This dismissal is part of a long-standing social stigma and has led to the broader field of UAP investigation being dismissed as lacking rigor and unworthy of serious investment.

A rigorous analysis of anomalous observations should not only preserve all relevant data, regardless of perceived credibility, but also rate detection events by their level of credibility. Two elements correlate with the credibility of a UAP observation: the training of human observers and the amount, diversity, and grade of sensor observations (collectively: technological capability). Both are typically the lowest for the public, the highest for the military, and between these extremes for law enforcement and civil aviation personnel. Operational credibility scales, including a composite detection-scenario scale and a human-observer rating system, are provided in *Appendix J: Observation credibility rating scale for frontline operations*. The scales are designed as shared vocabulary for downstream analysis. The credibility of an observer, whether human or sensor, has direct consequences for how much evidence is needed to reach a given confidence threshold. Figure 5 illustrates this 'sensor shortcut': to exceed ninety-nine percent certainty on the leading hypothesis from a skeptical prior, dozens of independent civilian eyewitness reports are required, whereas just several fused multi-sensor detections suffice. The numbers in this figure use heuristics from the forensic science literature (e.g. [16]), where we rate a civilian witness as providing weak evidence, a trained observer as moderate evidence, and a multi-sensor event as strong, starting from a highly skeptical prior of 1×10^{-6} for

the hypothesis. This is an illustrative example[9] but the qualitative conclusion is robust: Bayesian updating rewards evidence quality exponentially rather than linearly. As such, investing in calibrated detection infrastructure is not merely preferable; it is the most impactful action available.

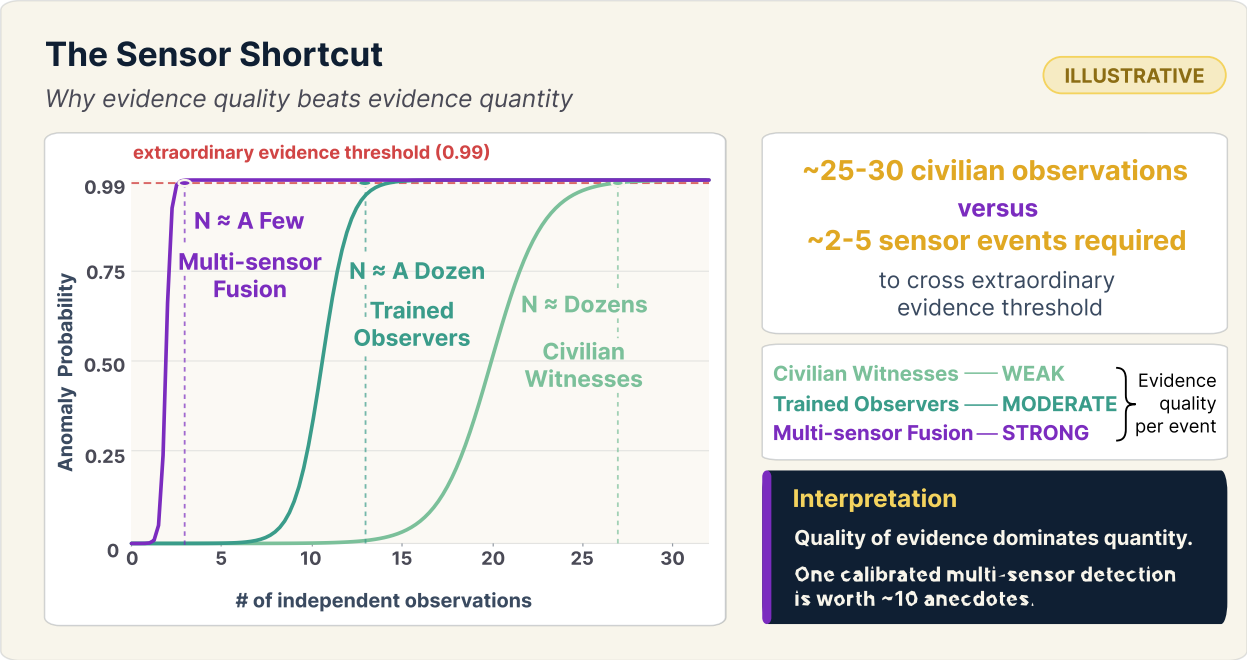

Figure 5: The 'sensor shortcut' is to improve evidence quality over quantity in Bayesian UAP identification.

From Explanation to Better Detection: The Observer Education Feedback Loop

A systematic effort to explain resolved UAP cases to the public creates a positive feedback loop for detection quality. When observers, particularly untrained ones (ratings 1 and 2 on the frontline credibility scale, see *Appendix J*: Observation credibility rating scale for frontline operations), are educated on prosaic causes behind commonly reported aerial phenomena (satellite constellations, atmospheric optics, drone swarms, classified test platforms), they develop better mental models for distinguishing the mundane from the genuinely anomalous. This raises the signal-to-noise ratio of incoming reports and focuses analytical resources on cases that most warrant investigation. The same principle applies to trained observers at higher credibility ratings, who benefit from reference frames that account for rapidly evolving aerospace technologies, including those that are classified and therefore indistinguishable from truly anomalous phenomena to even well-trained eyes.

This educational effort must acknowledge that the boundary between "advanced technology" and "anomalous" is not static. The current UAP landscape is almost certainly a heterogeneous mix of misidentified prosaic events, advanced or classified human-made technologies, and a residual set of genuinely unexplained phenomena. Transparent explanation of resolved cases preserves the significance of the unresolved while sharpening the collective ability to isolate the truly anomalous signal. By closing the loop between investigation outcomes and observer education, the CUF can progressively elevate baseline observer competence across all categories.

[9] Analysts assigning different likelihoods will reach different thresholds.

Hotspots and Observation Bias

Spatial clustering of UAP reports is a familiar feature of the public record. Sightings concentrate in the American West, along the Atlantic seaboard, in the Pacific Northwest, and on coastlines bordering restricted military airspace. The temptation is to read these clusters as evidence of where the phenomenon occurs. A 2023 Bayesian regression of 98,724 public UAP reports across the conterminous United States from 2001 through 2020 [17], found instead that reports correlate with where the sky is easiest to see and where aerial traffic is densest.

The methodological implication is sharp: spatial clustering is, in part, a map of observation opportunity rather than of phenomenon density. Any geographic-pattern claim must be corrected for observer density, sky-view potential, and traffic before it can be treated as evidence about the phenomenon itself. Observer bias is a measurable confounding factor, present in every human report, that can be modeled and subtracted rather than treated as disqualifying. The same logic applies to temporal clusters around news events, military exercises, and astronomical phenomena.

The CUF accounts for this explicitly. Before any spatial or temporal clustering pattern is treated as evidence about the phenomenon itself, the framework requires that observer density, sky-view potential, and traffic exposure be characterized and corrected for. A hotspot that survives that correction carries genuine evidential weight. One that does not is a map of observation conditions, not of anomalous activity.

Sensor Capabilities and Challenges

Technological sensors extend detection and measurement capabilities beyond the limits of unaided human perception. These instruments enable detection, tracking, and characterization of objects and phenomena across a wide range of conditions, including at long range, in darkness, through obscurants, and across portions of the electromagnetic spectrum invisible to the human eye. Table 7 summarizes sensing capabilities that are relevant to characterize an airborne target; each is described in detail in *Appendix D: Sensor Capabilities – Observables, Modalities, and Limitations*, alongside the sensor modalities that detect them. (Established infrastructure is covered by *Appendix C: Existing surveillance, sensing, and reporting infrastructure*)

Table 7: Sensing capabilities to characterize airborne targets.

Type	What it tells you	Key sensors
Visual-thermal	Shape, size, color, heat signature	Cameras, infrared / FLIR
Kinematics	Position, speed, altitude, heading, acceleration	Radar, LiDAR
Propulsion signatures	Engine exhaust, sound, air disturbance	FLIR, acoustic sensors
Composition	Material type (metal, gas, fabric, etc.)	Hyperspectral imager
RF emissions	Radio signals, transponder identity, control links	AIS, ADS-B, spectrum analyzer
Magnetic anomaly	Disturbance in the local magnetic field	Magnetometer

These observables are rarely available together. As such, the remainder of this section examines three structural consequences: spectral composition as the oft-missed modality, the fragmentation of detections captured, and the fusion necessary to compensate for these limitations.

The Case for Hyperspectral Sensors

Spectral imaging sensors are largely absent from the aerial platforms most likely to encounter UAP. Fighter aircraft such as the F-35 and F/A-18 carry advanced sensor suites that fuse radar, electro-optical, and infrared data, but these are optimized for threat detection and tracking, not for material identification. Similarly, c-UAS platforms rely on radar and EO/IR sensors sufficient for quick threat/no-threat decision making but yield no information about material composition. UAP identification has not historically generated the operational requirements that drive sensor integration on either fighter or c-UAS platforms.

Deploying spectral imaging in these operational scenarios presents non-trivial technical challenges, including detection range trade-offs with instrument aperture and integration time, illumination dependency, complexity of real-time data processing, and platform integration constraints (sensor size, cooling, weight, and power). However, recent military R&D efforts [18] targeting miniaturized hyperspectral sensors for small UAS, as well as early flight demonstrations [19] of spectral payloads on tactical UAS and manned aircraft, suggest these challenges are tractable and comparable in complexity to those already solved for existing FLIR and IRST systems. The recommended first step is to fund the development of a Concept of Operations (CONOPS) and engineering requirements specifically addressing spectral sensing for UAP identification, and enabling conceptual designs and costing for integration across relevant aerial platforms.

Detection by Accident, Evidence in Fragments

Because detections originate from systems built for other missions, each data point captures only the fraction of an event its mission requires: a defense radar fixes position and velocity but reveals nothing about composition; an infrared targeting system produces striking imagery but cannot bound range. The most compelling cases involve several simultaneous modalities, yet these are precisely the cases whose data is least often assembled into a standardized package, with classification limiting validation in military contexts and stigma suppressing it in civilian ones. The result is an evidentiary record built from mismatched fragments.

Anomaly or Artifact? Ruling Out Non-Anomalous Explanations

Most sensor records of UAP events are serendipitous, unexpectedly captured by instruments calibrated for other missions, in environments not chosen for the observation. The NASA UAP Independent Study Team identified poor calibration, missing metadata, and absent baselines as the central data deficit. Before an event is treated as anomalous, it must survive a first-pass assessment against the ordinary explanations that can mimic an anomaly: sensor faults (calibration errors, processing artifacts, and environmental interference), deliberate adversarial effects (jamming and spoofing), and the canonical signal-processing pipeline itself, which routinely discards the very returns that matter. Common ‘hygiene’ of a signal-processing pipeline includes Moving Target Indicator (MTI) and Doppler filters to suppress near-zero radial velocities, Constant False Alarm Rate (CFAR) algorithms to censor sub-threshold targets, and tracker gates to reject kinematically improbable plots, producing a synthetic blindness in which UAP-like signatures exist in raw data but never reach the display, as illustrated in Figure 6, which contrasts what the sensor actually captured with the cleaned-up picture the operator is shown. Machine-learning detectors do not inherently escape this: a model trained on conventionally labeled returns learns the same rejection rules, reproducing the blindness in less transparent form unless built to flag anomalies rather than match

familiar traces. A verifiable anomaly is what survives all of these checks and still shows signatures across different sensor types. *Appendix E: Diagnostic Triage for Sensor Faults, Interference, and Deception* catalogs the principal classes of explainable effect, the signatures by which each is recognized, the diagnostic questions that distinguish it, and the corresponding mitigations.

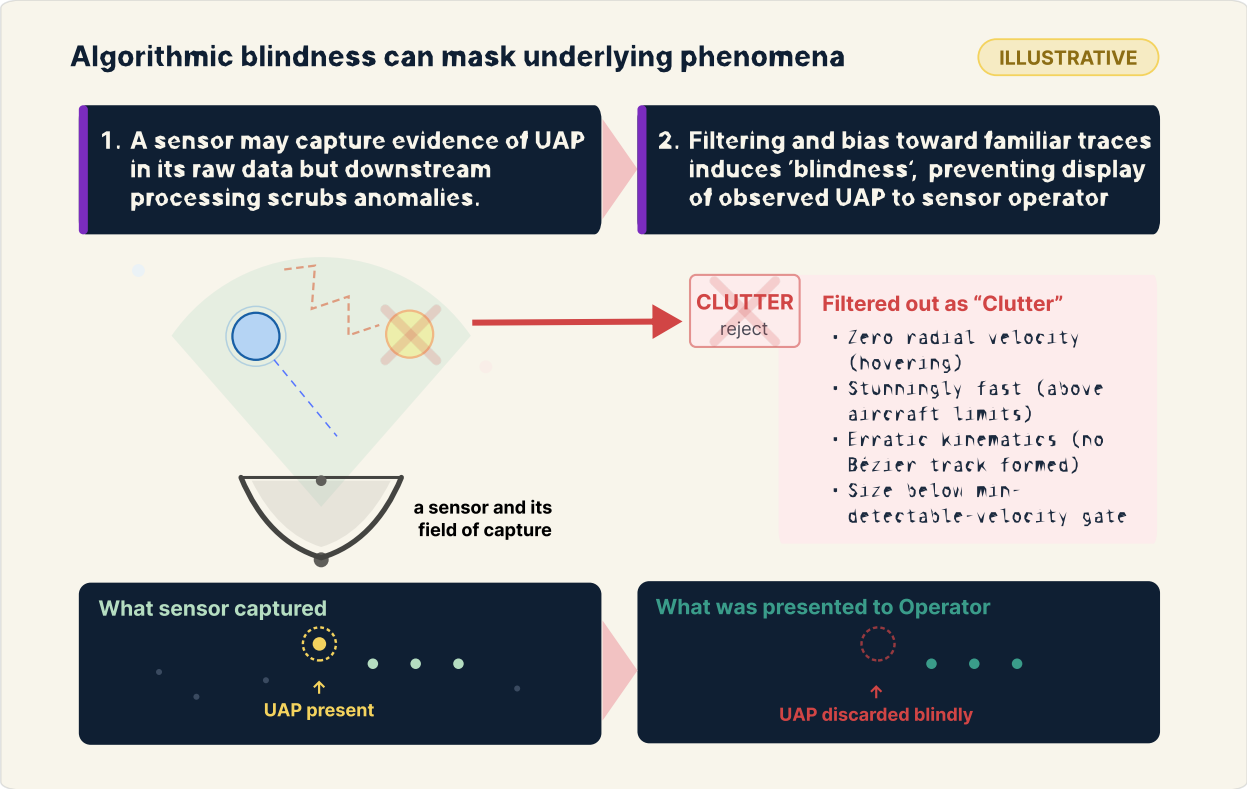

Figure 6: Algorithmic blind spots can manifest when legacy radar-processing pipelines filter-out low-radial-velocity or kinematically improbable returns, producing synthetic blindness in which UAP-like signatures exist in raw sensor data but never reach the tactical display.

Determining whether any of these underlies a given detection requires ancillary sensor data that typically exists but is rarely released for independent analysis: calibration status, maintenance logs, firmware version, and raw telemetry, along with records of how the same sensor behaved on known, prosaic objects. These are generally recorded but often not retained or not made accessible[10] and may be irretrievably lost as a result. Establishing detection-record standards that bundle this ancillary information with the primary observation would substantially increase the credibility and analytical utility of sensor-based UAP reports.

[10] This is owing to classification, retention policies, or the simple absence of any requirement to preserve them.

Multi-Sensor Fusion

No single modality resolves a UAP detection, as each leaves gaps the others can fill. Multi-sensor fusion combines them to constrain the hypothesis space: an event registered across radar, optical, and infrared simultaneously rejects most artifact and interference modes that would mimic a single channel. Fusion also enables triangulation across spatially separated stations, which converts apparent angular motion into three-dimensional kinematics and corrects for forced-perspective effects.

The NASA UAP Independent Study Team identifies multi-sensor, well-calibrated data as paramount for advancing the field. Operationally, the Galileo Project commissions all-sky infrared arrays paired with visible cameras, RF, acoustic, and magnetometer sensors at fixed sites [20]. This multi-modal architecture is what makes it possible to discriminate between explanatory hypotheses, thus building confidence in genuinely anomalous explanations only after artifact and interference explanations have been independently ruled out across sensors.

Identifying Unknowns

UAP identification has historically been approached as retrospective case resolution: identified or unidentified, resolved or unresolved. That binary model, inherited from Project Blue Book (1952–1969) and continued through AARO, is useful for archival reporting but poorly suited to three real-world demands.

Table 8: Historical identification frameworks compared.

Framework	Era	Key categories	Primary use
Project Blue Book	1952–1969	Identified, insufficient data, unidentified	USAF case sorting
Hynek classification system	1972	Nocturnal lights, daylight discs, radar-visual, close encounters (1st–3rd kind)	Civilian and academic encounter classification
ODNI / UAP Task Force	2021	Airborne clutter, natural phenomena, USG/industry, foreign adversary, other	Intelligence analytical classification
AARO	2022–present	Same as ODNI plus resolved/unresolved labels	U.S. government UAP investigations
Confronting Unknowns Framework (proposed)	2026	Artifact, natural, unclassified tech, classified tech, unknown	Operational decision-making and scientific sensemaking

First, many events develop over time and involve partial, multimodal evidence. A binary label applied at a single point discards the structure of the evidence. Second, operational decision-making cannot wait for definitive attribution. A probability distribution over explanatory hypotheses is more useful than a pending "unresolved" label. Third, cumulative scientific analysis requires structured representations of uncertainty that can be updated

as new data, methods, or context become available. A case that resists resolution at first pass should carry a living record of uncertainty rather than a closed file.

The alternative: treat identification as a function. Given a flagged event record, produce a ranked list of explanatory hypotheses with current probability assignments, explicit about the assumptions behind them, the dominant uncertainties, and what additional evidence would most change the assessment. Rather than collapsing to a vote that terminates as "unresolved," the assessment updates across the hypothesis set as evidence arrives—a provisional distribution rather than a verdict.

Anomaly Resolution: From Binaries to Probabilities

CUF proposes five explanatory hypotheses to form a set that is mutually exclusive and, by construction, collectively exhaustive, allocating probability for explanations not yet articulated. The set is designed to be revised; as evidence accumulates, a hypothesis may be split, merged, or added, and probability that once sat in H5 may migrate to a newly named category. This is a feature and is how the framework represents that the space of possible explanations is not 'mentally foreclosed.'

Table 9: CUF explanatory hypotheses.

Type	Icon	Hypothesis	Description
H1	⊞	Data or Sensor Artifact	The apparent event is primarily a product of sensor behavior, processing error, or interpretation failure. Examples: parallax, lens flare, radar multipath
H2	≈	Natural Physical Source	The event reflects a known, real physical phenomenon from atmospheric, astronomical, oceanic, or geophysical causes. Examples: birds, ball lightning, meteors, mirage
H3	⊠	Human-Made Physical Source (unclassified)	The event reflects a real object consistent with conventional or commercially accessible technology. Examples: space/air debris, satellite, balloon, crewed and uncrewed aircraft ("drone")
H4	Δ	Human-Made Physical Source (classified)	The event reflects a real object associated with restricted state or defense activity. Examples: allied or adversary test program
H5	✶	Unknown Physical Phenomenon	The event involves a real physical phenomenon not adequately explained by H1–H4. H5 functions as the open residual: it holds probability for explanations the current hypothesis set does not yet name. Examples: novel natural phenomena, non-human intelligence, residual unknowns

Three design choices distinguish this hypothesis space. Artifact (H1, ⊞) is an explicit top-level hypothesis, not merely an attribute of a report, because artifact classification is always in tension with the most exotic explanations: for H5 to rank high, H1 must rank very low. An event should be beyond reasonable doubt not a sensor artifact before extraordinary explanations are entertained.

Human-made technology is bisected into unclassified (H3, ⊠) and classified (H4, Δ): military sensor systems disproportionately encounter classified programs: a collection bias with direct legal and operational implications for stable identification.

The space of hypotheses affords prosaic explanations a natural home: a potential UAP later recognized as a civilian aircraft falls squarely into H3, and categorizing known objects and phenomena is as valuable as categorizing unknowns, because it establishes a baseline for what “normal” looks like.

Two qualifications anchor the hypothesis space. First, anomalous and unknown are not the same thing. A phenomenon can be genuinely anomalous yet already understood by someone. A classified program (H4, Δ) is the clearest case, but the principle is general: knowledge is unevenly distributed, and what is unknown to a frontline operator may be known elsewhere. The operational goal is therefore to move cases toward resolution by whoever holds, or can develop, the relevant knowledge, resisting the treatment of 'unknown' as a permanent property of the event. Second, the boundaries between categories are crisp in principle but can be fuzzy in practice, because the line between 'natural' (H2, ≋) and 'unknown' (H5, ✶) tracks the provisional state of physical science. A phenomenon classed as natural may later prove novel, or one classed as unknown may resolve to an unusual but conventional process. Reclassification across these boundaries is expected as understanding improves; the framework treats it as the system working, not failing.

Approaching identification with a probabilistic mindset means maintaining a distribution over all five hypotheses that reflects current evidence—not collapsing prematurely to a single answer. The starting distribution is not necessarily uniform: context carries information, and a prior that ignores it does not improve objectivity. In the ideal case, evidence raises one hypothesis decisively: the functional equivalent of a "Resolved" case. In practice, many incidents land in an intermediate state, with two or three hypotheses each holding 20–40% probability. These are the hardest cases to respond to and explain, but the ones that most benefit from honest probabilistic representation, as well as the ones where targeted collection has the highest expected payoff.

As a further example, Figure 7 illustrates our suggested approach, which assigns different probabilities to different causes. A UAP ‘trilemma’ is presented, in which there is a tension of supporting multiple competing explanatory hypotheses: H4 (classified human-made technology), H5 (unknown phenomenon), and even H2 (natural phenomenon) may explain the observation given the data, though none of these hypotheses alone can be assigned with high (e.g., >80%) confidence.

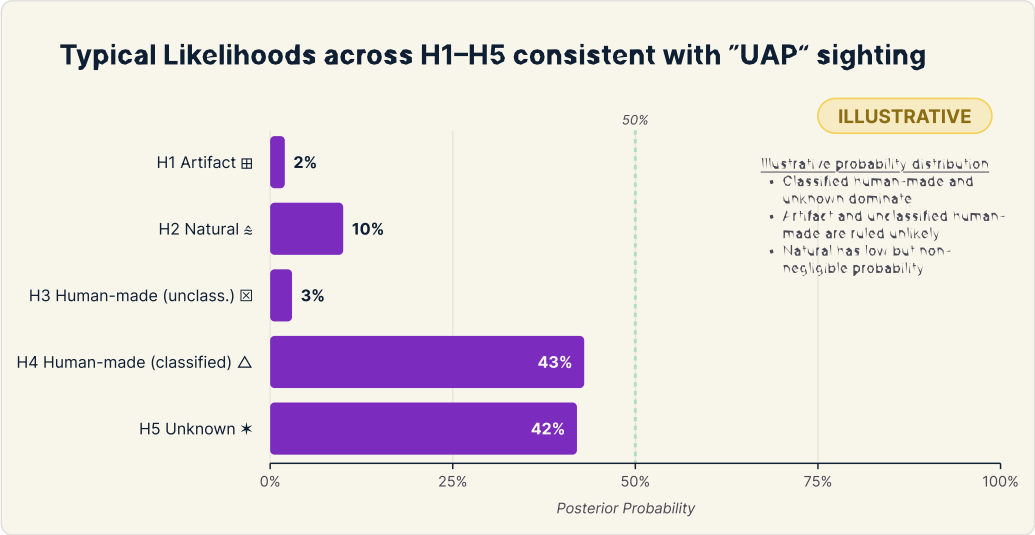

Figure 7: An example UAP 'trilemma' of CUF hypotheses H1–H5.

Functioning as a loop, the CUF ensures that communication failures feed back into detection and identification, and institutional responses are architected in a manner to generate signals more consequential than the original events. Feedback paths matter as much as the forward path: identification feedback refines detection parameters; communication feedback refines the vocabulary and delivery of identification outputs; the accumulated record of cases builds institutional knowledge for all stages.

Five Steps from Data to Ranked Hypotheses

A disciplined identification workflow runs in five steps. Each step is procedural for the operator and auditable for a reviewer; the framework's probabilistic claims rest on the discipline of the earlier steps being done first.

1. **Integrity check.** Before any inference, establish what kind of record is in front of you. Verify provenance, calibration, and synchronization; look for the signatures of processing artefacts. The goal at this step is not to confirm the data is anomalous. The goal is to confirm the data is what it claims to be.
2. **Kinematic and signature analysis.** With clean data, estimate position, velocity, acceleration, and trajectory, each with explicit uncertainty bounds. Characterize additional observables—compositional, acoustic, electromagnetic, and magnetic signatures or environmental effects. Separate what the sensor measured from what an analyst inferred.
3. **Context correlation.** Run the event against the conventional explanations: air traffic, weather, astronomical objects, satellite passes, launch records, and restricted-area operations. Most anomalous reports resolve at this step.
4. **Multi-sensor consistency.** When the event survives context correlation, test whether independent sensors and observers agree on the basic facts. Agreement across modalities raises confidence that the signal is physical. Agreement alone does not make the signal anomalous.
5. **Hypothesis scoring.** Score the H1–H5 hypotheses against the evidence, record the dominant uncertainties, and route the case: archive, monitor, re-task for additional collection, or escalate for restricted correlation.

To illustrate how context shapes the result: in a wargame applying this workflow to a simulated low-altitude incursion over a civilian area near a military installation, the two human-made explanations (unclassified and classified technology, H3 and H4) together dominate, with classified technology (H4) alone accounting for roughly half the total. Running the identical evidence against a restricted military-airspace scenario shifts the result further toward H4. Nothing the sensors recorded changed between the two runs; only the context (and, therefore, the starting assumptions) differed. Context carries information; ignoring it does not improve objectivity.

A Note on Method: Probability in Emergency Management

Bayesian statistics are a method for reasoning under uncertainty. It starts by stating what is believed before new evidence arrives, then revises that belief as evidence comes in, and rather than forcing a single yes-or-no verdict, it produces a range of possibilities each weighted by how likely it is. For policymakers, the appeal is practical: it requires analysts to put their assumptions in writing, makes any disagreement easy to trace to its source, and lets an assessment to be updated as new facts emerge instead of being scrapped and rebuilt from scratch.

Because of these qualities, the method is established across high-stakes fields where decisions cannot wait for complete data: emergency management situation awareness [21], early outbreak detection [22], wildfire [23] and earthquake forecasting, and intrusion detection in critical infrastructure networks [24], among others [25], [26].

The implications for disaster response are direct: responders rarely have clean or complete data, yet must commit resources before the picture resolves, and Bayesian methods let an assessment begin with whatever is known and sharpen as observations accumulate.

Critically, these same response systems are inherently dual-use and portable to new domains. The sensor-fusion and situation-awareness infrastructure built for emergency response and critical-infrastructure protection, discussed in earlier sections, already performs the core task UAP assessment requires, and would demand little fundamental modification: the analyst still weighs competing explanations, records the reasoning behind each, and updates as evidence accumulates.

The way this paper handles uncertainty is deliberately kept simple. We name a fixed set of explanations, assign each a rough starting probability based on context, and adjust them up or down as evidence comes in. We made this choice for transparency: a decision-maker, a congressional staffer, and an analyst can all look at the same numbers and pinpoint where they disagree, such as the starting assumptions or how well the evidence fits each explanation.

We want to be explicit about what the simple version leaves out. Two limitations matter most. The first: we treat the list of explanations as fixed during any single analysis, even though the framework is meant to be revised between analyses. More advanced methods handle this head-on: allowing the number of explanations to grow as evidence accumulates, holding probability in reserve for explanations no one has named yet and creating a new category only when the data genuinely call for one. Our open residual (H5) is the plain-language version of that idea, a deliberate reserve of probability set aside for the possibility that the current categories are incomplete, but

a fuller treatment would let that reserve actually generate new, named explanations rather than leaving it to an analyst's judgment to spot when one is needed.[11]

The second limit: we commit to a single set of starting assumptions for each context. A different tradition works with a whole range of plausible initial assumptions at once and favors decisions that hold up well across the entire range—often the more honest approach when reasonable people disagree about where to start. We use the single-set approach because policy audiences need one legible picture, not a cloud of competing ones. But the confidence of any single result depends on starting assumptions that other careful analysts could reasonably dispute.

The practical takeaway is modest and important: the framework's outputs are inputs to human judgment, not replacements for it. The numbers are only as good as the explanations we thought to name, our reading of the evidence, and the assumptions we started from, all three of which are revisable. Future work should build the open-ended version of the hypothesis space formally, so that the reserve category does not merely sit as a placeholder but actively proposes new explanations as evidence grows.

Anomaly Analysis: Artificial Intelligence for Unknowns

Recent advances in artificial intelligence create an opportunity to augment expert-driven identification across the resolution workflow described above.

Large Language Models (LLMs) and multimodal models can assist by normalizing heterogeneous reports, extracting structured information from narrative text, correlating records against external databases, surfacing likely artifact modes, triaging cases, and summarizing uncertainty for different audiences. They can also generate a provisional distribution over the H1–H5 hypotheses. Critically, AI makes the probabilistic framework itself more accessible: Bayesian reasoning has traditionally required specialist statistical expertise, but AI tools can do the analytical heavy lifting of integrating evidence streams, computing likelihoods, and updating estimates, while presenting results as natural-language summaries and ranked hypothesis lists. This affords frontline practitioners to apply rigorous probabilistic reasoning without deep statistical training.

Multimodal LLMs offer a specific capability relevant to UAP analysis: processing visual data (images, plots of physical quantities) using few-shot, in-context learning. Where traditional machine learning requires hundreds of thousands of labeled examples, multimodal LLMs can identify anomalies from a handful of data points, a property well suited to a domain plagued by data scarcity. Over-simplifying: "given these 5 images of confirmed UAP and these 5 images of conventional drones, reason about the next image and tell me if it's likely to be a UAP or a drone, and why." The same few-shot approach is already being adopted in industry (e.g., manufacturing defect detection) and applies to any data that can be rendered as an image, including sensor-data plots. A mere 20-second military infrared video can be decomposed into timestamped multimodal observations: image frames, apparent motion vectors, thermal contrast patterns, and scene metadata. Even 'small' UAP datasets can be enriched along multiple dimensions (including visual, kinematic, thermal, temporal) to partially bridge this data gap.

[11] The idea of recursive hypothesis generation has been studied extensively in the statistics literature. See [27], [28] for foundational sources.

> *Multimodal LLMs can identify anomalies from a handful of data points, a property well-suited to a domain plagued by data scarcity.*

Testing these Multimodal LLMs for UAP analysis requires no new technology or large datasets: a small set (tens to hundreds) of well-selected, validated examples plus access to state-of-the-art models suffices for early experimentation. However, these systems are vulnerable to false confidence, inconsistent reasoning, hallucination, and non-transparent failure modes, and their inference cost makes real-time or large-scale use impractical today, so current results may be insufficient for operational deployment. Yet the pipelines are portable to better models as the technology evolves and could soon exceed the performance and explainability of traditional methods that require massive training datasets—and which do not yet exist for UAP.

Dual-use pathways using existing and emerging detection infrastructures

Much of the required detection infrastructure already exists; it is just not under that label as such. A mature ecosystem of counter-UAS, environmental monitoring, and industrial surveillance systems is already built to continuously detect, classify, and respond to small, low-altitude, and hard-to-identify aerial targets.

This sensing capability extends beyond the air domain. Offshore and industrial sites increasingly deploy sensor systems that include sonar for underwater detection (e.g. [29], [30]), identifying divers, submersibles, and anomalous objects near critical infrastructure. In maritime settings, combining these acoustic and sonar inputs with radar, optical, and RF sensing is a natural extension for UAP detection.

In the security sector, modern counter-drone radars (e.g. [31], [32]) explicitly target objects most relevant to UAP reporting: low-flying objects that are hard to detect by radar and move with irregular flight patterns. These systems increasingly read the fine motion signatures of an object's moving parts using MTI/Micro-Doppler techniques to distinguish birds, drones, and helicopters.

Environmental systems offer parallel capabilities. Bird-monitoring radar systems used in wind-farm operations (e.g. [33], [34], [35]) continuously track and classify small airborne objects under noisy, real-world conditions, integrating radar, optical sensors, and real-time analytics to track movement and trigger responses like turbine shutdowns.

Atmospheric platforms sensing such as methane detection and anomaly mapping tools (e.g. [36]) can help explain common misidentifications such as thermal inversions, gas emissions, or optical distortions. More broadly, the field is converging on large-scale sensor networks, drone integration, and AI-driven analysis for observing complex, dynamic systems (e.g. [37], [38]).

NASA, NOAA, the U.S. Space Force, and private-sector space companies are already building out the sensing, cataloging, and traffic-coordination infrastructure needed to operate in an increasingly congested near-Earth environment (e.g. [38], [39], [40]). As satellite constellations, launch activity, and orbital debris grow, the technical problem is no longer simply detecting objects, but integrating heterogeneous measurements, maintaining custody, filtering known objects, and sharing safety-relevant information across civil, military, and commercial users. These efforts provide a useful dual-use model for spaceborne anomaly detection: not a dedicated UAP observatory, but a federated architecture that combines public data systems, debris measurements, commercial sensing, and operational space-domain-awareness capabilities.

Across these domains, the bottleneck is integration and standardization, not novel sensing. A credible detection framework for unknowns would emerge from federating existing industrial and environmental systems into an open, multi-modal pipeline that both flags anomalies and rules out known objects under operational conditions.

Part III: Respond & Explain

What To Do, What To Say?

1. How did institutional communication break down during the New Jersey wave, and what can we learn from the breakdown?
2. Why do anomalous aerospace events keep producing the same communication failures across decades?
3. How can institutions communicate explicit uncertainty without amplifying speculation?
4. What does an aligned response look like in the first hours of the next incident?

Part III: Respond & Explain turns from objects to institutions. Communication failures recur across decades of responses to anomalous events. This Part examines that breakdown, and what a disciplined response, one that conveys uncertainty without feeding speculation, would look like in the first hours of the next incident.

Learning from Today: New Jersey Media Melee

As of the publication date of this paper, additional information regarding this incident is still being released into the public domain. However, the incident highlights the communication challenges of anomalous aerospace events. When there is no central institutional voice to speak clearly about unknown (or classified) events, the information void is quickly filled with conspiracy theories, disinformation, and speculation which can quickly escalate into public panic. There has been a century of challenges around government and media communications regarding anomalous aerospace events dating back to the Cold War. These include files now on the public record stating a formal policy to deny, stigmatize and debunk anomalous phenomena.

The lack of formalized acknowledgement of anomalous phenomena produced four interlocking failures: no vocabulary for explicit uncertainty, an active stigma against reporting, dismantled inter-agency protocols, and an information environment that now outpaces institutional response. The following section summarizes and breaks down this breakdown step-by-step.

- On December 8, 2024, Ryan Herd, the mayor of Pequannock Township, circulated a letter to Governor Phil Murphy. Within days, twenty-one mayors across Morris County had signed it. “Our efforts to address these concerns have been hindered by the lack of information available to us,” the mayors wrote. “This situation is untenable.” The letter was prompted not by the objects but by weeks of procedural non-answers from every level of government.
- The governor’s office convened a classified briefing at the state emergency operations center in Ewing Township within forty-eight hours. Roughly 185 mayors attended, alongside representatives from the State Police, FBI, DHS, and DoD. The briefing produced the opposite of clarity. Colonel Patrick Callahan of the New Jersey State Police acknowledged that officials did not know what the objects were, even as they insisted there was no threat. “How do you know they’re not a danger if you don’t know what it is?,” Mayor Ryan Herd remarked.

- Craig Robertson, a retired Army major and counter-UAS specialist who had served in the Pentagon's Asymmetric Warfare Group, offered his expertise to the State Police and FBI directly. The initial reception was positive, but "every time I tried to dive deeper, the conversation just went cold," commented Robertson. The institutional posture Robertson observed was the same one that functions in classified environments but becomes corrosive when applied to domestic airspace: "they don't really owe answers to civilian people."
- Herd's question exposed the logical incoherence of simultaneous "no threat" and "we don't know" claims. Robertson's experience demonstrated that reflexes designed for classified environments suppress useful expertise in domestic incidents. The Ewing briefing showed that assembling every relevant federal agency in one room does not produce answers when none of those agencies has the detection architecture, identification methodology, or communication authority to provide them.

When Different Explanations are Circulated, It Encourages Conspiracy Thinking

Viewed from an intelligence officer's perspective, the force of different concurrent narratives may encourage a breakdown in social cohesion in response. While that may be useful in other settings, for marshalling a useful response these are to be avoided.

Table 10: New Jersey drones: four explanatory narratives in the media

"Adversary"	**"Misidentified"**
- "Iranian Mothership" - "Foreign (e.g. Chinese/Russian) Spy Drones"[12] [42]	- Misidentification of airplanes, helicopters, stars - Hobbyist or commercial drones - "Mass Hysteria"
"Us"	**"Genuinely Unidentified"**
- "Loose Nuke/Dirty Bomb Search" - FAA-approved military exercises or research flights - Unacknowledged, classified U.S. military activity	- UAP - Novel atmospheric or environmental effect

The coexistence of these narratives demonstrated that no institutional actor had the credibility, information, or communication infrastructure to narrow the hypothesis space in real time.

[12] Note: Multiple federal agencies have explicitly stated there is no evidence of foreign involvement.

From Watching to Lasering: The Escalation Ladder

Journalists reporting from the field during the ensuing media melee of the New Jersey drones incident in 2024 [8] documented three categories of community response, each escalating in risk:

A. **Observation.** Neighborhood watches organized to track the objects. Citizen scientists deployed personal electro-optical sensors (the Nightcrawler Research system) and shared data with both law enforcement and the press [43], [44].
B. **Interception.** Local police and private individuals launched personal drones to photograph or intercept the objects.
C. **Neutralization.** Individuals shone high-powered lasers at the objects, striking several commercial aircraft, a federal offense and prompting FBI response.

Open-hardware platforms such as the UFO Data Acquisition Project [45] complement institutional systems by providing standardized, low-cost sensor packages that citizen scientists can deploy for persistent monitoring; UFODAP rigs integrate visible, infrared, and radio-frequency sensors with GPS-timestamped data logging.

The escalation from observation to interception to armed engagement is what an information vacuum produces. Communities improvise when institutions go silent, and improvisation in this domain includes lasers aimed at commercial aircraft. Rebuilding communication infrastructure is the precondition for not repeating the pattern.

The conventional model treats communication as the end of the pipeline: an event is detected, identified, and then communicated. The New Jersey case inverts that sequence: each institutional response generated new signals more consequential than the original detection and the inversion is traceable step-by-step as follows:

- starting in late November 2024, residents across Morris County called their mayors about low-flying objects;
- the mayors contacted the county sheriff, State Police, and governor's office. The answers were procedural and inconclusive: no confirmed operator, no identified launch site, no clear line of authority;
- that vacuum, weeks of non-answers, was the signal that prompted twenty-one mayors to send their letter on December 8.

The letter was not a response to contradictory statements but rather a response to the absence of any substantive statement at all and what followed accelerated the cycle:

- the classified briefing at Ewing Township, intended to reduce uncertainty, instead produced a new and more powerful signal: the officials assembled in the room, representing every relevant federal agency, could not explain what was in the airspace they were responsible for;
- Herd's subsequent media tour amplified that signal to national reach within hours.

Then the contradictory cascade followed:

- The state senator's emergency call (December 10);
- the FBI/DHS joint statement (December 12);
- "Shoot them down" (Trump, December 13);
- "Nothing nefarious" (Biden, December 17);
- cumulative 22 FAA flight restrictions (December 18).

Each response contradicted or undercut the last. By mid-December, the dominant information environment was no longer just about unidentified aircraft but also about institutional failure. As Scaduto wrote, "Reassurance without explanation is a debased currency: it circulates briefly, then collapses."[8]

The response-to-signal loop operated on two timescales simultaneously. On the fast timescale (hours to days), individual statements became raw material for media narratives. Van Drew's Iranian mothership claim, issued [15] and retrac[46]46] within 48 hours, seeded a threat narrative that persisted online for weeks after retraction. On the slow timescale (weeks to months), accumulated institutional incoherence generated legislative action: New Jersey's A5712, Vermont's H.654, renewed federal proposals. The objects triggered the first response. Every response after that was triggered primarily by prior responses.

This dynamic is not unique to New Jersey. In February 2024, at a routine budgetary meeting of the Pennsylvania Emergency Management Agency, state representative Ben Waxman asked PEMA Director Randy Padfield about UAP tracking near nuclear power plants. Padfield confirmed that past reports came through county 911 calls, that tracking was "really under the FAA's purview," and that most sightings were "unfounded, or they're attributable to some other mechanism." State representative Jordan Harris interjected: "You said 'most.' So what about the un-most?" Padfield's answer trailed into procedural language. In Pennsylvania, as in New Jersey, the institutional response communicated more about the system's limitations than about the phenomena it was asked to explain.

The implication for framework design: communication cannot be treated as the terminal stage of a linear pipeline. When institutional communication fails, the resulting vacuum does not merely leave the public uninformed; it actively degrades the next detection cycle by redirecting political pressure toward premature closure (the Leavitt statement) or performative action (calls to shoot down the objects) rather than better sensing.

> *How do you know they're not a danger if you don't know what they are?*

Structural Failures: A Century of Anomaly Miscommunication

The public communication failures that accompanied the New Jersey drone incursions were not novel. They were the predictable product of four structural failures, each traceable to a specific historical origin.

Failure 1: No vocabulary for explicit uncertainty. The pattern was established early in multiple incidents, in which an anomalous aerospace event drew official attention and the institutional response was premature closure rather than honest uncertainty.[13] Since then, public UAP communication has often been forced into a false binary: either authorities know what something is, or they insist it poses no threat. Missing is a durable institutional vocabulary for the honest middle ground: we detected something, we do not yet know what it is, and we are still investigating. Many later communication failures stem from that gap.

Failure 2: Legacy stigma suppresses reporting. A declassified 1953 CIA scientific review recommended a formal campaign to stigmatize the topic and reduce public interest; the resulting social and professional penalty for reporting anomalous observations has persisted for seven decades (see *Appendix I: Historical precedents in anomalous-event communication*).

Failure 3: Missing/Dismantled inter-agency protocols. When the New Jersey drones appeared, the White House, FAA, DHS, FBI, and DoD each issued statements without a shared factual basis because no inter-agency protocol had ever been rebuilt. Similarly, the closure of the U.S. Air Force's Project Blue Book; the program left no successor coordination mechanism and actively stigmatized the creation of one (see *Appendix I: Historical precedents in anomalous-event communication*). With no trusted official channel, civilian groups like MUFON and military whistleblowers filled the vacuum. Their reports accumulated in a gray zone: too persistent to ignore, but too stigmatized and institutionally unsupported to resolve with adequate rigor.

> *Officials can say 'we know what it is' or 'there is no threat,' but no institutional language exists for the honest intermediate: we have detected objects we cannot yet identify.*

Failure 4: **The information environment outpaced institutional capacity.** The contemporary phase began in December 2017, when the *New York Times* revealed the Advanced Aerospace Threat Identification Program (AATIP), a Pentagon office tasked to study anomalous aerospace events [49]. Between 2022 and 2025, Congress held four public hearings on UAP, with classified sessions alongside. In 2025, the documentary *The Age of Disclosure* [6] featured 34 current and former government officials. Some described direct knowledge of recovered objects and reverse-engineering programs. Senator Marco Rubio offered more guarded framing: "We have people with very high jobs...that are either A: liars, B: crazy, or C: telling the truth." The documentary's contested reception—27% critics, 91% audience on Rotten Tomatoes—illustrates a credibility gap. Also, while the AARO office

[13] For example, at Roswell in 1947, the Army Air Field announced the recovery of a "flying disc" and then retracted it as a weather balloon within a day [47]. In the 1966 Michigan sightings, an Air Force consultant attributed a wave of credible reports to "swamp gas," a dismissive ruling that did not fit many of the accounts and that the investigator himself later disowned [48].

was set up to provide a factual account of the government's history with UAP, its first historical report released in 2024 was widely criticized [50] as filled with mistakes and factual errors.

By the time the New Jersey incursions occurred, the information environment bore no resemblance to the one in which the Robertson Panel could plausibly manage public perception through institutional gatekeeping. The 1997 Phoenix lights took weeks to reach national awareness; a comparable event today goes viral within a day. The institutional communication cycle (investigation, inter-agency coordination, legal review, press clearance) operates on a timescale of days to weeks. By the time an official statement is issued, the narrative has been set by whomever spoke first, regardless of whether they had evidence.

The four structural failures traced above operated simultaneously during the New Jersey incident and the inter-agency gap was the most operationally visible. No standing protocol exists for inter-agency communication during anomalous aerospace events, analogous to protocols for natural disasters, disease outbreaks, or terrorist attacks [8]. Worse, the vocabulary gap compounds the coordination gap. Officials must choose between misleading certainty ("no threat") and silence. Both erode trust. The New Jersey case, in which a retired counter-UAS specialist offered his expertise and was frozen out, demonstrates that a penalty structure created by the 1953 Robertson Panel remains active. Stigma reduces the volume and quality of reports reaching analysts; thinner reporting yields weaker detection and weaker identification; and officials are then asked to communicate around the silence their own system produced.

Unified Incident Command and Threat Planning

The Incident Command System (ICS) is the standard U.S. framework for organizing emergency response across agencies and jurisdictions. It is used for natural disasters, industrial accidents, terrorist attacks, search-and-rescue operations, cyberattacks, public-health emergencies, and major planned events. Its purpose is to reduce confusion by establishing clear command, standardized terminology, shared situational awareness, and defined responsibilities for operations, planning, logistics, finance, and public communication.

ICS begins with an *Incident Commander*, usually from the agency with immediate jurisdiction. As an incident grows, command can transfer or expand. When several agencies or jurisdictions have authority, ICS can form a *Unified Command*, allowing them to set common objectives while preserving their statutory roles. For large or geographically dispersed incidents, an *Area Command* or Emergency Operations Center can coordinate multiple incident commands and allocate resources.

The system is built to scale. A local emergency can remain local, while a major disaster may involve state emergency management, FEMA, the National Guard, and, if needed, U.S. Northern Command under Defense Support of Civil Authorities. Counterterrorism or mass-casualty events may bring together local police, emergency medical services, federal investigators, and intelligence agencies. These cases show that ICS can accommodate overlapping authority, sensitive information, and even classified channels when there is a recognized incident requiring organized response.

The New Jersey drone incursions fell into a more ambiguous category. Local officials, law enforcement, airports, military installations, and federal agencies all had stakes in the situation, but the events were not publicly treated as a confirmed emergency or credible threat. Federal messaging repeatedly stated that there was no evidence of a national-security or public-safety threat, and many sightings were later attributed to lawful drones,

aircraft, or misidentifications. Because the incidents did not clearly become a declared emergency, terrorist incident, aviation disaster, or confirmed hostile drone operation, they did not trigger a visible full ICS/ National Incident Management System (NIMS) activation.

The response remained agency-specific. Local police gathered reports and handled public concern. State officials coordinated with law enforcement channels. The FBI collected tips and investigated possible criminal activity. The FAA managed airspace and safety restrictions. DHS and DoD provided assessment or technical support where appropriate. Military installations operated under separate force-protection authorities. But there was no clearly identified Incident Commander, Unified Command, Joint Information Center, or shared incident action plan for the overall event.

The result was a command-and-communication gap. Airspace authority sat largely with the FAA; investigation with the FBI and law enforcement; mitigation authority with limited federal actors; military bases under separate defensive authorities; and state/local officials left managing public concern without full control over relevant tools or information. In a hurricane, wildfire, chemical spill, or confirmed attack, these overlapping authorities would likely be integrated through ICS/NIMS. In the drone case, because the incursions were not officially treated as a credible threat, coordination occurred through ad hoc inter-agency channels rather than a formal emergency-response architecture.

The policy lesson is that major drone waves and ambiguous aerial incidents need clearer ICS/NIMS triggers. Even before hostile intent is confirmed, officials may need a scalable structure for reporting, evidence preservation, airspace coordination, classified-to-unclassified information sharing, public messaging, and escalation. The New Jersey episode therefore illustrates not a failure of ICS itself, but the absence of a clear playbook for applying ICS to ambiguous low-altitude aerial events.

Moving Ahead: Communicating Uncertainty with Clarity

- How can government press and analytical offices share information across agencies during incidents involving anomalous phenomena, given differing classification authorities and legal constraints?
- How can information move across national borders during incidents involving anomalous phenomena, when allied and partner governments operate under different classification authorities, disclosure norms, and legal frameworks?
- Where should sharing happen at the analytical level rather than only the public-affairs level, and what existing channels including aviation-safety bodies, air-defense arrangements, and intelligence-sharing agreements could carry that coordination across agencies and across borders?
- What would an evidence-informed approach to timely public communication look like? What governance structures ensure accuracy while operating at the speed the information environment demands?
- Can AI-assisted analysis tools improve the speed and consistency of public-facing information synthesis during anomalous events?
- What can UAP whistleblower cases teach about designing legal protections and incentive structures for reporting anomalous observations?
- Is the current posture of transparency (FOIA, congressional hearings) helping or hindering effective information management? Under what conditions does partial disclosure increase rather than decrease public confusion?

Before Disclosure, Accountability

Any future disclosure of new information about anomalous phenomena will be received in the context of the history traced above. The U.S. government's credibility on this topic carries specific debts that precede and constrain any forward-looking communication strategy.

Before the scientific community or public can be expected to accept new information on this topic, these past activities require formal institutional acknowledgment. Trust requires demonstrated accountability, not promised accountability, and not future accountability. The historical record contains documented actions for which no official accounting has occurred, and that unresolved ledger will shape the reception of any future disclosure regardless of content.

> *Trust requires demonstrated accountability, not promised accountability, and not future accountability.*

Implications by Audience: Communications

Part III's lesson is that the response, not the object, did the damage. This section reads that lesson through the people who must act on it, each facing the same communication and coordination problem from a different position.

For policymakers. Part III's central finding is structural: domestic airspace sits at the intersection of FAA, DHS, FBI, and DoD authorities with no standing inter-agency protocol for anomalous events, and ICS/NIMS was never triggered in New Jersey because the events did not cross any single agency's threshold for "credible threat." A scalable ICS/NIMS playbook for ambiguous low-altitude aerial incidents, clear Incident Commander designation, Joint Information Center authority, and classified-to-unclassified information bridges, is the policy artifact this Part argues for most directly. Whistleblower protection language already drafted in prior UAPDA iterations should travel with any future disclosure framework; "Before Disclosure, Accountability" is the sequencing this Part proposes, not as principle but as precondition for the audience reception of any new disclosure.

For operators. The escalation ladder this Part documents, observation, interception, neutralization, is what an information vacuum produces at the community level. The operator implication is not about civilians; it is about what frontline communicators can do in the first hours of a similar event to prevent civilians from lasing commercial aircraft. Pre-drafted public communication templates that acknowledge detection, describe the current state of identification, and commit to a follow-up cadence would have changed the December 2024 cascade meaningfully. Public affairs officers at FAA, DHS, FBI, and DoD need a shared vocabulary for the honest intermediate between "we know what it is" and silence; that vocabulary is what does not currently exist.

For scientists & researchers. The four structural failures above are the empirical case for a research agenda that does not yet have an institutional home. The communication system around anomaly events has not been studied with the seriousness applied to the anomalies themselves. Specific lines of falsifiable work are visible from this material:

- **Trust dynamics under information cascades.** Risk communication is a mature field for pandemics, financial panics, and nuclear incidents; it has barely been applied to anomaly events. The 76-day arc between the first Picatinny lights and the Press Secretary's January 28, 2025 statement is a complete longitudinal case for studying how local-trust collapse propagates upward and outward.
- **Declassification cohort analysis.** Project Blue Book, the Condon report, Robertson Panel transcripts, and the AARO 2024 historical report exist as a corpus that no team has read systematically alongside contemporaneous press coverage. Comparing what was internally known with what was publicly said, document by document and year by year, is the load-bearing evidence base for Failures 2 and 4 (deliberate misdirection; whistleblower reprisal).
- **Conspiracy formation under information vacuums.** The empirical literature on conspiracy belief studies content (what people believe); it rarely studies the structural conditions, deliberate information suppression, that make alternative content available in the first place. Anomaly events with documented suppression are natural experiments for the latter, currently unexamined.
- **Disclosure-design science.** No published protocol exists for credibly releasing previously stigmatized information. The Church Committee is the closest historical analogue, but it has not been studied as a communication design problem, which choices in framing, sequencing, and venue made its findings durable where other releases did not.

These lines build empirical foundations for the recommendations in *Part IV: An Action Agenda for New Unknowns*. Without them, the disclosure architecture proposed rests on the convener's intuition.

For public communicators. This is the Part that speaks most directly to public communicators, and the implications are sharper here than elsewhere. Five practical norms emerge from the New Jersey case. Distinguish anomaly from response, most of what went viral in December 2024 was about the institutional response, not the objects. Resist closure pressure on both sides; the "no threat" cascade and the "Iranian mothership" cascade were the same failure mode in opposite directions. Treat retractions as ongoing news, not as event-closure; Van Drew's retraction reached a fraction of the audience the original claim did. Use the H1–H5 vocabulary publicly, "where the evidence currently points" is more honest and more durable than "officials say." And maintain the distinction between misinformation, disinformation, and malinformation in a domain where ground truth is genuinely uncertain; premature debunking is its own failure mode.

Diagnostic Markers for the Next Incident

If the analysis in this paper is correct, the next anomalous aerospace event of meaningful scale is likely to follow the same sequence as the four cases documented above (New Jersey in 2024, Langley Air Force Base in 2023, the Denmark drone wave in 2025, and Barksdale Air Force Base in 2026). The following are diagnostic markers to signal if the response is aligned with the framework.

A. **Detection fragments across agencies.** Watch for whether pipelines tuned to suppress non-standard signatures discard relevant data before any human sees it. If the surviving fragments never get correlated, the integration step still has no owner.
B. **Identification stalls in the binary.** If the event is labeled "unresolved" or "under investigation" rather than carrying a probability distribution over named hypotheses, the framework's central recommendation has not been adopted. The label discards the partial evidence the framework is designed to accumulate.

C. **A communication vacuum opens in the first seventy-two hours.** If no inter-agency protocol exists to coordinate the initial public statement, multiple agencies will say different things. The difference tends to become the story.
D. **The response becomes a larger signal than the original detection.** If political pressure moves toward premature closure or performative action, the institutional response itself becomes the event the public remembers.

If the Tier-1 recommendations in *Part IV: An Action Agenda for New Unknowns* are in place, the same four mechanisms run in reverse: a coordinated initial statement within twenty-four hours; honest language for genuine uncertainty; standardized event preservation that enables re-analysis. The response-becomes-signal loop still operates, but the institutional response reduces the vacuum rather than filling it.

Part IV: An Action Agenda for New Unknowns

What to Build Before the Next Incident

1. What scientific infrastructure does anomaly research need, and how should its discoveries be governed?
2. Which detection and identification capabilities deliver the most value per dollar?
3. What must be in place before the next incident so the response is not improvised?
4. How do institutions rebuild public trust before they need it?

Confronting future unknowns requires investment today. Anomalous-phenomena research offers genuine scientific upside in materials science, atmospheric physics, and sensor design (among other areas), and it carries equally genuine risks in biosecurity, cybersecurity, and national security. Both the upside and the risk point to the same instrument: a technology governance roadmap that names the decision points for classification, controlled disclosure, and dual-use oversight.

Part I's *"Crisis Playbook"* addressed what to do in the first hours of an incident; this Part addresses what to build before the next one, organized as four tiers of action and four supporting priorities:

Table 11: Immediate Actions and Priorities

Actions	Priorities
1. Create named research funding categories at NSF, DOE, and NASA.	1. Establish dedicated observatories.
2. Develop a NIMS/ICS playbook for ambiguous low-altitude incidents.	2. Develop sensor fusion.
3. Hold a 'Church Committee'-style accounting of past information-management activities before any new disclosure framework is built.	3. Create open-source data platforms to standardize data collection, management, analysis, and reporting practices.
4. Engage the public.	4. Engage the public.

The Church Committee Model to rebuild public trust

Formally acknowledge and end past information management activities. Congress could hold hearings and formally acknowledge past activities of disinformation, whistleblower reprisals and other unethical activities conducted by U.S. Government in relation to anomalous phenomena going back to the 1940s.

This formal acknowledgement process may be modeled on the Church Committee Hearings [1], the 1975–1976 Senate investigation that publicly documented decades of intelligence abuses and produced lasting oversight reforms, and paired with whistleblower protections. These measures may help in rebuilding public trust in government prior to moving forward with any new policy for a more open and transparent communication on future incidents. These would work well with whistleblower protections, which have been included in previous iterations of UAP transparency legislation.

Inset B: The Church Committee is a model to account for past information-management activities.

Action 1: Support Science for a New Era

The scientific investigation of anomalous phenomena requires a well-funded, well-governed infrastructure that does not yet exist. Federal science agencies, universities, private philanthropy, and technology-governance institutions (NIST, CISA, FCC) each hold a piece of the puzzle; none holds enough alone. The opportunity is extraordinary: anomalous-phenomena research touches physics, biology, materials science, astronomy, earth science, and sensor engineering. The risk is commensurate. Without governance, the same discoveries that could unlock clean energy or hypersonic travel could introduce biosecurity, cybersecurity, or national-security hazards that no existing framework is designed to manage.

Identify Scientific Investigation Priorities & Funding Needs

- **Create Scientific Discoveries Road Map.** Prepare an analysis of key research questions, potential applications, and research pathways needed for discoveries. Studies of anomalous phenomena cover many areas of scientific investigation from physics, biological, materials, astronomy, planetary and earth science. The potential discoveries could have applications across many domains including clean energy, hypersonic travel, materials science, communications technology, neuroscience and more.
- **Establish dedicated research funding categories for anomalous phenomena studies.** Direct federal science agencies, beginning with NSF, DOE, and NASA, to create named program elements or cross-directorate initiatives under which research proposals on anomalous phenomena can be explicitly submitted, reviewed, and tracked. Currently, no federal science agency offers a competitive grant category for this research; investigators must frame UAP-relevant work under adjacent disciplines, rendering it institutionally invisible and reinforcing professional stigma. Peer-reviewed studies [51] have found that the availability of competitive research grants is the single most important factor that would unlock faculty participation. A formal category would provide a legitimacy signal for tenure and promotion decisions, enable systematic tracking of funding levels and research gaps, and establish civilian science funding infrastructure commensurate with the governmental attention this topic now receives.

- **Develop Research Needs Assessment and Funding Plan.** Conduct a full consultation with scientific organizations and other stakeholders on key research questions and discovery pathways. Prepare an action plan with potential government sponsors, scientific philanthropy and private funding sources that might be made available to fund each project.
- **Fund observational feasibility studies for anomalous phenomena detection.** UAP research presents a distinctive challenge: there is no predictive theory to guide where, when, or how to observe, and the phenomena appear to be rare and transient. Before committing to large-scale observational campaigns, agencies should fund systematic studies assessing which combinations of sensor technologies, geographic locations, and monitoring strategies would maximize the probability of capturing scientifically useful data at an acceptable cost. This includes evaluating existing infrastructure, such as weather radar networks, satellite constellations, and astronomical survey instruments, for untapped potential to detect anomalous events, as well as informing the design of purpose-built multi-sensor observatories. Such studies would establish the evidence base needed to make rational investment decisions about observational programs.
- **Establish research institutes and coordination mechanisms.** Identify potential performers of scientific investigations and coordinated mechanisms for funding and grants. Where appropriate, identify mechanisms for open-source database development and data sharing and potential creation of non-profit independent Focused Research Organizations (FROs) [52] that can coordinate inputs from researchers based at multiple institutions and across multiple disciplines.

> *Currently, no federal science agency offers a competitive grant category for frontier research.*

Establish Technology Governance

- **Clarify patent and IP treatment for UAP-derived technologies.** Policymakers should address how intellectual property law would apply to discoveries or technologies emerging from UAP research. If UAP are engineered artifacts, reverse-engineered technologies may raise prior-art or ownership problems. If they are natural phenomena, the underlying principles may not be patentable at all. Clarifying this framework early would reduce legal uncertainty and help determine whether private investment can realistically support UAP-related research and development, to include internationally-developed technologies and capabilities.
- **Set clear rules for compartmentalization, secrecy orders, and export controls.** Policymakers should clarify when UAP-related research, patents, materials, or reverse-engineering programs should remain classified, compartmentalized, restricted under secrecy orders, or subject to export-control regimes, or be on a pathway to be made available on a restricted access basis only or for open-source scientific investigations. This should include guidance on the degree of compartmentalization, oversight mechanisms, criteria for declassification or controlled release, and how existing frameworks such as the Invention Secrecy Act, Atomic Energy Act, ITAR/EAR controls, and defense-classification authorities would apply to potential breakthrough technologies. Operational practices for partial release of classified sensor data already exist. Released video can be masked to obscure sensor-specific artefacts so the imagery is shareable without disclosing the collection method. These practices should be standardized across agencies, not improvised case by case.

- **Clarify guidance on private sector data sharing with government agencies.** Clarify what data sharing policies and incident reporting requirements will govern private research initiatives, particularly when there is a public health, safety, or national security threat.
- **Develop a technology risk and opportunity assessment.** Develop an assessment of risks that could result from the investigation, experimentation, and dissemination of findings of studies of anomalous phenomena and their mitigations. This assessment should also consider the opportunity offered by potential technological and scientific breakthroughs, and how to integrate public purpose, while also rewarding private investment, in the dissemination of such breakthroughs.
- **Build a technology governance roadmap.** Develop a forward-looking governance framework for managing potential discoveries arising from scientific investigations of anomalous phenomena, with particular attention to findings that could carry biosecurity, cybersecurity, or national security risks. The roadmap should identify decision points for classification, controlled disclosure, and dual-use oversight, and should address discoveries originating from both government-funded and private research initiatives.

Action 2: Enhance Detection and Identification Capabilities

Detection and identification capabilities must serve two purposes simultaneously: frontline operators who need answers in minutes, and researchers who need reproducible data that survives peer review. Academic and government scientists, independent research organizations, private sensor companies, and the operators themselves all contribute. Open-source data and high-quality peer-reviewed studies will improve anomaly detection across all domains and advance the scientific understanding that underpins credible policy.

Develop Dedicated Observatories for UAP Scientific Investigations

Observatory investment is the single highest-priority investment for transforming UAP research from anecdotal reporting into calibrated, reproducible science. The dedicated observatories described in *Appendix E: Diagnostic Triage for Sensor Faults, Interference, and Deception* and the sensor-tier framework in *Part II: Detect & Identify* provide the technical foundation; the policy actions below translate that foundation into funded programs.

- **Site a baseline network in low-coverage areas.** Existing surveillance systems reveal where sensors are, but not necessarily where events occur. Reviewing the historical incident record for sparsely monitored regions would help distinguish observation bias from genuine activity patterns and identify where new sites would provide the greatest coverage gains. A statistically designed network of calibrated sites in sparsely monitored regions would provide the control data needed to distinguish genuine spatial patterns from observation bias, while extending data acquisition into the corridors least observed by current systems.

Create Next Generation Sensors Capabilities for UAP Observation

- **Integrate hyperspectral sensing into current sensor platforms.** Support integration of hyperspectral imaging sensors onto platforms that currently carry FLIR systems. This is the single most achievable

investment that adds materials compositional capabilities to operational sensor suites to distinguish (bird, drone, balloon, etc.).

- **Develop next-generation sensors for UAP observation.** Invest in novel sensor capabilities designed after the observational requirements and concept of operation of typical UAP incidents. Repurposing existing sensors, engineered for different observation targets, has limited returns for phenomena that manifest differently than most known technologies.

Build Standardized Data Collection & Classifiers

- **Develop a verified taxonomy of anomalous events.** Compile an unclassified system for categorizing the types and characteristics of phenomena reported in the airspace, since reported UAP are likely a mix of human-made, natural, and other phenomena. A common catalog would give analysts, operators, and the public a shared language for describing what is observed, and it could be built from both public and classified information without requiring the declassification of the underlying data.[14]
- **Build a data discovery engine.** Develop a tool that, given the approximate location and time of an observation, identifies what monitoring systems were observing that same volume of space. (Including weather radar, satellite imaging, ADS-B, AIS, radiosonde, see *Appendix C: Existing surveillance, sensing, and reporting infrastructure*.)

Develop Open-Source Data Sharing for Scientific Investigations

- **Publish open detection architectures.** Follow the model established by the Galileo Project [53] and publish detailed engineering specifications that provide an auditable record for the generated data and can inspire the further development of new observational concepts and capabilities. The platform could be used by research to develop reproducible studies, which is a prerequisite for highly credible, peer-reviewed research.

Invest in AI-assisted Models for Anomaly Resolution

- **Develop AI-assisted identification of anomalous events.** Develop anomalous incident analysis pipelines based on multimodal Large Language Models that can detect anomalies in sensor data including how human-AI collaboration should be structured in safety-critical settings.
- **Develop machine-learning tools for UAP investigation.** Develop object-recognition algorithms to distinguish conventional drones and UAP for use in frontline operations. The cost decomposition matters. A UAP detection-and-classification pipeline built atop existing foundation models is a $1–10M effort. A UAP-specific foundation model trained from scratch could be a $100M+ effort[15] and risks rapid

[14] This descriptive taxonomy is distinct from the explanatory hypothesis space used to identify an event. The taxonomy standardizes how an observation is described; the H1-H5 hypothesis space (described in *Part II: Detect & Identify*) is the set of candidate causes over which an analyst distributes probability for a single case. Description is upstream of explanation, and keeping the two separate prevents a label for what was seen from hardening into a verdict on what caused it. Standardized description in turn strengthens the identification, response, and explanation stages.

[15] A substantial fraction of this cost would be gathering training data.

obsolescence against the rapid evolution of commercial multimodal models. As *Part II: Detect & Identify* explains (See *"Anomaly Analysis: Artificial Intelligence for Unknowns"*), a pipeline built on commercial foundation models inherits each new generation of those models, while a model trained from scratch is frozen at its training date and falls behind. We recommend the pipeline-first path.

- **Develop probabilistic models of anomalous events.** Replace the resolved/unresolved labeling system with one that preserves ranked explanations and structured uncertainty rather than collapsing each case to a single verdict. The CUF hypothesis space (H1–H5) is a deliberately simple starting model; three directions would strengthen it. First, setting the initial probabilities for each explanation transparently, and adjusting them across contexts, factoring-in how a civilian airport differs from a restricted military range. Second, weighing and combining evidence of uneven quality from radar, infrared, acoustic, and human sources. Third, and most valuable: letting the list of explanations grow as evidence accumulates, so that a genuinely novel event prompts a new category rather than being forced into the catch-all (H5). Methods to do this exist and are well established in machine learning.

Action 3: Improve Aerospace Incident Readiness & Response

The New Jersey incursions demonstrated that no incident-command framework exists for ambiguous low-altitude aerospace events. Congress, the NSC, DHS, FAA, federal and state law enforcement, counter-UAS operators, and frontline responders all have roles, but no protocol assigns them. Thoughtful public communications and standardized event reporting require the kind of advance preparation that currently exists for pandemics, nuclear incidents, and financial crises but not for drone waves.

Conduct Federal & State Emergency Management Policy Reviews

- **Review the homeland security Incident Command System (ICS).** Review how FEMA approaches 'drone waves' under its current policies and protocols and advise on key policy gaps and support needs to better manage future incidents.
- **Clarify how the FAA issues flight restrictions.** Review how the FAA issues flight restrictions in response to reports of drone waves or reports of anomalous sightings and how best to balance air safety with air traffic disruptions.
- **Bridge the decide-and-respond gap.** Evaluate which decision architectures are appropriate for events where identification yields a probability distribution rather than an attribution. Advise on how rules of engagement, airspace management, and inter-agency coordination adapt to probabilistic uncertainties.
- **Build data tools to create a universal operational picture**. Create a data capture, classification and management system where any reporting or event is fused with ADS-B, Remote ID, FAA flight data, weather, radar if available, 911 calls, and critical-infrastructure maps.
- **Map detection blind spots and place sensors to close them.** Study the historical record for sparsely populated and lightly monitored regions to estimate how much of the current picture reflects where sensors and observers already are, rather than where events actually occur. Use that analysis to prioritize sensor placement in the zones the record cannot currently see.

- **Support state-level coordination.** New Jersey's A5712, Vermont's H.654, and Connecticut's H.B.5422 represent an accelerating movement of state responses. While constructive, they risk fragmenting a problem that requires federal coherence. Congress should establish federal-state coordination that incorporates state-level research and reporting into a national system.

Support Frontline Operators Responding to Anomalous Events

- **Create a drone-incursion FEMA/NIMS/ICS playbook.** Review how drone waves and anomalous events are treated as incidents under NIMS/ICS and develop a playbook for incident commanders and first responders.
- **Fund and train local c-UAS response teams on anomalous phenomena.** Create training for c-UAS response teams on anomalous phenomena and mainstream the training across military, law enforcement and private security services operators qualified to operate c-UAS systems.

Develop Interagency Coordination and Communication Protocols

- **Establish inter-agency communication protocols for anomalous events.** Direct the NSC to develop and exercise inter-agency protocols for anomalous aerospace incursions, analogous to existing protocols for natural disasters and terrorism. The New Jersey incident demonstrated that no such protocol exists, as opposed to extensive existing playbooks for a pandemic, nuclear incident, or financial crisis.
- **Clarify management of classified information.** Clarify the command structure and information management process for creating and communicating classified information during response to events involving anomalous phenomena.
- **Develop standardized event data-preservation infrastructure.** Mandate reporting and retention standards that preserve raw data, metadata, sensor calibration state, and chain of custody. AARO's intake processes reduce events to narrative summaries insufficient for re-analysis [54].
- **Develop a public communication template for anomalous airspace events.** Pre-draft templates that acknowledge detection, describe the state of identification, and commit to follow-up. This directly addresses the vocabulary gap: officials need prepared language for the honest intermediate between "we know what it is" and silence.
- **Strengthen aviation safety reporting.** Expand NASA's ASRS or establish a parallel channel for anomalous event reporting by commercial pilots and air traffic controllers. The 2023 NASA UAP Independent Study [55] recommended this; it has not been implemented.

Action 4: Engage the Public

Public trust is the medium through which every other recommendation in this paper travels. If institutions cannot communicate honestly about what they detect and what they do not yet understand, the information vacuum will be filled by speculation, conspiracy, and improvisation. Media organizations, journalists, online platforms, scientific bodies, healthcare institutions, Congress, and government public-affairs officers each shape the information environment; none controls it.

Build Trusted Information Environments

- **Map the current information environment.** No systematic study has charted the sources, intermediaries, and amplification pathways through which information about anomalous phenomena reaches the public. Such a study would identify which experts journalists consult, which platforms host the most active discourse, and where misinformation originates and propagates. Without this map, any communication strategy operates blind.
- **Train the communicators.** Three groups need structured preparation. Government public affairs officers at the White House, DHS, FAA, and DoD need protocols and vocabulary for events that are detected but not identified. Journalists and trust-and-safety teams at social media platforms (Meta, X, Reddit, YouTube) need briefings on the distinction between misinformation, disinformation, and malinformation in the specific context of anomalous aerospace events, where ground truth is genuinely uncertain and premature debunking can be as damaging as premature confirmation. Scientists who speak with the media and advise policymakers during anomalous events also need public communications training and support on how to communicate unknowns.[16]
- **Build an open-source information portal for public education.** A public-facing clearinghouse (e.g. Propublica's Rx Inspector [57] or Cochrane Review's Plain Language Summaries (PLS) of medical evidence [58]) could aggregate information from official sources, peer-reviewed research, and credible detection projects. The goal: a persistent, citable, evidence-graded resource that journalists, legislators, and researchers can reference when an incident occurs. The portal could include information such as information on understanding sensors, expert interpretation of declassified information and imagery, Q&As on current events, as well as rapid-fire lessons on deep-fake debunking and information quality assessment, as well as fact-checking best practices and outreach for all ages.

Provide Health Services and Sensemaking Support

- **Prepare healthcare providers.** Individuals who report close encounters with anomalous phenomena frequently describe physical symptoms, psychological distress, or both. In the United Kingdom, the nonprofit UnHidden provides training to NHS providers on supporting patients reporting extraordinary experiences. No equivalent exists in the United States. Primary care physicians and mental health professionals need clinical guidance that neither pathologizes reporting nor validates specific interpretations. Protocols to deal with physical effects most likely due to exposure to ionizing or microwave radiation may be useful to deal also with other emerging threats, such as direct-energy weapons.
- **Engage sensemaking communities.** The experience of anomalous events and findings of scientific studies involving anomalous phenomena are often interpreted through the lens of teachings of religion, indigenous traditions and spirituality. Additionally, many findings of UAP scientific studies could challenge long held beliefs across many scientific fields from physics, earth science, anthropology, neuroscience and more. These communities need meaningful consultation and engagement in the design, participation, and dissemination of studies, for study findings to be broadly accepted.

[16] C.f. the International Science Reserve (ISR) [56], established to assist governments in a crisis like a pandemic, volcanic eruption, et cetera.

Implications by Audience: Action Agenda

The agenda above is substantive. Below is an arrangement for the people who must carry it out.

For policymakers. First, establish a named research funding category for anomalous-phenomena studies at NSF, DOE, and NASA: peer-reviewed work has identified this as the single most important unlock for faculty participation [51], and the absence of a named category is what currently makes the field institutionally invisible. Second, direct the NSC to develop and exercise inter-agency communication protocols for anomalous aerospace incursions, on the analogy of pandemic, nuclear-incident, and financial-crisis playbooks; this is the same Tier 1 lever converged on in *Part I: The Problem* and *Part III: Respond & Explain*. Third, pursue a Church Committee–style formal acknowledgment of past information-management activities, paired with whistleblower protections already drafted in prior UAPDA iterations [3]; the sequencing matters because any forward disclosure will be received against an unresolved historical ledger.

For operators. The agenda for operators converges on standardization. A drone-incursion FEMA/NIMS/ICS playbook for incident commanders and first responders. Training for c-UAS response teams on anomalous phenomena specifically, mainstreamed across military, law enforcement, and private security. Expansion of NASA's ASRS, or a parallel channel for anomalous-event reporting by commercial pilots and air traffic controllers, which the 2023 NASA UAP Independent Study [55] recommended and which has not been implemented. And a universal operational picture tool that fuses ADS-B, Remote ID, FAA flight data, weather, radar, 911 calls, and critical-infrastructure maps; this is an engineering project, not a research project.

For scientists & researchers. Part IV's research agenda is the most concrete in the paper. The high-leverage items: observational feasibility studies to identify which sensor-location-strategy combinations maximize useful data per dollar; hyperspectral CONOPS development; multimodal LLM identification pipelines with explicit attention to false confidence and hallucination failure modes; probabilistic models calibrated against the H1–H5 hypothesis space with attention to how priors should differ across operational contexts; and Focused Research Organization structures [52] for cross-institutional coordination. The agenda is intentionally heterogeneous because the underlying phenomena, on current evidence, are heterogeneous.

For public communicators. Part IV is specific about the communicator agenda. Map the current information environment, sources, intermediaries, amplification pathways, because no systematic study has been done and any strategy will operate blindly without that map. Build a public information portal that aggregates official sources, peer-reviewed work, and credible detection projects into a citable, evidence-graded resource. Train three communicator populations: government public affairs officers, journalists and platform trust-and-safety teams, and the scientists who advise the public during anomalous events. And engage healthcare and sensemaking communities upstream of the next incident, primary care physicians and mental health clinicians need clinical guidance that neither pathologizes reporting nor promotes specific interpretations.

The Most Important Change to Make...

The Tier 1 protocol is the only recommendation in this paper upon which the other recommendations depend. Hyperspectral payloads, the H1–H5 hypothesis space, the public information portal, and every operator-level shift named in Part II run through the inter-agency seam. The 76 days between the Picatinny event and the Press Secretary's "no national security threat" statement are the operational definition of why the protocol needs to exist before the next incident.

An Argument That Does Not Depend on the Answer

Our framework is deliberately agnostic about what anomalous aerospace events ultimately are. It sets aside questions of non-human intelligence, exotic propulsion, and novel physics. Whatever the objects turn out to be, the institutional infrastructure required to confront them is the same: better detection, identification under uncertainty, credible communication.

The investment is justified by demonstrated failure, not by any assumption about what the objects are. Suppose the unknowns prove mundane. The infrastructure improves aerospace safety, operational awareness, and public trust. Suppose instead the unknowns prove extraordinary. The infrastructure provides the evidentiary foundation without which extraordinary claims cannot be responsibly evaluated. The first step does not change. ■

Appendices

This page intentionally left blank.

Appendix A: Glossary

A5712. New Jersey Assembly Bill 5712, signed January 12, 2026, by Governor Phil Murphy as P.L. 2025, c.269. Establishes a state Center for the Study of Unidentified Aerial Phenomena with approximately $3.5 million in appropriations, including $2.5 million in research grants.

AARO. All-domain Anomaly Resolution Office. U.S. Department of Defense office established in 2022 to investigate UAP across air, sea, space, and transmedium domains; reports through ODNI channels and issues annual consolidated reports to Congress.

AATIP. Advanced Aerospace Threat Identification Program. Pentagon office that studied anomalous aerospace events from 2007 to 2012 with approximately $22 million in funding; publicly revealed by the *New York Times* in December 2017.

AAWSAP. Advanced Aerospace Weapon System Applications Program. Defense Intelligence Agency program (2008–2010) that preceded AATIP, contracted to Bigelow Aerospace and producing the DIRD technical report series on advanced propulsion and related topics.

ADS-B. Automatic Dependent Surveillance–Broadcast. Cooperative surveillance technology in which aircraft broadcast position, altitude, velocity, and identity via transponder. Objects detected on radar but absent from ADS-B feeds are common candidates for further investigation.

AESA. Active Electronically Scanned Array. A phased-array radar architecture on modern fighter aircraft including the AN/APG-77 (F-22) and AN/APG-79 (F/A-18E/F), enabling rapid beam steering and simultaneous multi-target tracking.

AFGSC. Air Force Global Strike Command. U.S. Air Force major command headquartered at Barksdale AFB, responsible for the bomber leg of the nuclear triad and most U.S. ICBM forces.

AI. Artificial intelligence. Systems performing tasks that typically require human cognition, including perception, reasoning, and classification. In CU26, AI refers to: 1) emerging capabilities in machine-learning and multimodal LLM systems to be used for sensor-data triage, anomaly detection, and probabilistic identification; 2) a human-origin form of complex non-human intelligence, hypothesized to be useful as an investigable, interrogatable proxy for other forms of non-human intelligence.

AIM-9X. Air Intercept Missile 9X "Sidewinder." Short-range infrared-guided air-to-air missile carried by U.S. and allied fighters; cited in escalation-ladder discussions of intercept options.

AIS. Automatic Identification System. Global vessel-tracking transponder system used in maritime surveillance; relevant for ruling out ship misidentification in coastal and over-water UAP events.

Anchoring. A cognitive bias in which decision-makers weight a first plausible explanation too heavily, biasing subsequent analysis. Identified in the Crisis Playbook as a decision trap to be checked through structured workflow gates.

AN/APG-77. The AESA radar carried by the F-22 Raptor. Provides long-range air-to-air detection and tracking with low-probability-of-intercept characteristics.

AN/APG-79. The AESA radar carried by the F/A-18E/F Super Hornet. Provides simultaneous air-to-air, air-to-ground, and electronic-warfare functions.

Antwerp incursion. Reported drone incursion over the Belgian port of Antwerp during the November 2025 Belgian drone wave; Belgium announced plans to install an air-defence system at the port by 2027.

Article 4. The provision of the North Atlantic Treaty allowing any NATO member to request consultations when its territorial integrity, political independence, or security is threatened. Invoked by Estonia in September 2025 after Russian MiG-31 airspace violations.

Artifact (H1). The explanatory hypothesis space attributing an apparent event primarily to sensor behavior, processing error, or interpretation failure (e.g., parallax, lens flare, radar multipath). The paper treats H1 as an explicit top-level hypothesis rather than a report attribute.

ASRS. Aviation Safety Reporting System. Confidential, voluntary reporting system administered by NASA for the FAA, processing approximately 100,000 pilot and ATC reports per year.

Asymmetric Warfare Group. A former U.S. Army unit (2006–2021) providing operational advice on irregular and emerging threats; alumni include the retired Army counter-UAS specialist whose offered expertise during the New Jersey incident was declined.

ATFLIR. Advanced Targeting Forward-Looking Infrared. Targeting pod on U.S. Navy aircraft providing infrared imagery; source of several widely circulated UAP videos.

Atomic Energy Act. U.S. statute (1954, as amended) governing the development, regulation, and disposition of atomic energy and nuclear materials; classifies certain weapons-design and reactor information as "Restricted Data." Cited alongside the Invention Secrecy Act and ITAR/EAR as one regime potentially applicable to breakthrough technologies derived from UAP study.

Authority bias. A cognitive bias in which decision-makers defer to the highest-ranking voice in a room rather than the best-informed one. Identified in the Crisis Playbook as a decision trap.

Availability bias. A cognitive bias in which the most recent, vivid, or dramatic explanation is weighted disproportionately. Identified in the Crisis Playbook as a decision trap.

AWACS. Airborne Warning and Control System. The E-3 Sentry aircraft providing long-range airborne radar, command and control, and battle management; cited in the Langley response as a platform deployed against the unidentified incursions.

Baltic Sentry. NATO maritime mission launched in January 2025 to protect undersea cables, telecom links, and pipelines in the Baltic Sea following damage to seabed infrastructure.

Bardufoss. Norwegian Air Force station and civil airport in Troms; reported flight disruptions linked to drone sightings during the September 2025 Denmark drone wave.

Barksdale AFB. U.S. Air Force base in Bossier Parish, Louisiana, home to the 2nd Bomb Wing (B-52H) and headquarters of Air Force Global Strike Command. Experienced unauthorized drone incursions beginning March 9, 2026.

Bayesian inference. A statistical method in which prior probabilities for a set of hypotheses are updated to posterior probabilities as new evidence arrives, using Bayes' theorem. In the CUF, the mechanism for ranking the H1–H5 hypotheses as sensor data, contextual information, and expert analysis accumulate.

B61. The B61 family of low-yield U.S. tactical nuclear gravity bombs. Referenced in nuclear-asset and force-protection contexts associated with bases experiencing drone incursions.

Berlin Brandenburg Airport. Germany's principal Berlin-area international airport (BER); briefly suspended takeoffs and landings on October 31–November 2, 2025 after an unknown object was reported near a Bundeswehr (German military) helicopter hangar, and again for nearly two hours after a late-evening drone sighting.

Blue Book. See Project Blue Book.

Bremen Airport. German civil airport in Bremen; temporarily suspended takeoffs and landings on November 2, 2025 after a drone was spotted nearby, with at least one flight allegedly prevented.

Brussels Airport. Belgium's principal international airport (BRU); repeatedly closed during the November 2025 Belgian drone wave, including more than 50 cancellations on November 4 and roughly 500 passengers overnighting in the terminal.

Brønnøysund. Norwegian coastal airport; subject of an Avinor-confirmed drone observation inside the restricted zone on September 28–29, 2025 during the Denmark drone wave.

BVLOS. Beyond Visual Line of Sight. The capability of an unmanned system to operate beyond direct visual contact with its operator; a regulatory and detection challenge for civilian and counter-UAS authorities.

C2. Command and control. The systems, processes, and authorities through which commanders direct forces; "C2 links" denote the radio data path between a drone and its operator.

C-17. The C-17 Globemaster III strategic airlifter. Cited in the December 2024 Stewart Airport incident in which an unauthorized UAS approached within 25–50 feet of a C-17.

C-UAS. Counter-Unmanned Aircraft Systems. Sensors, effectors, and procedures designed to detect, track, identify, and neutralize unauthorized drones. Federal C-UAS authority in the United States is concentrated at DOJ and DHS, with expansion proposals pending.

Camp Pendleton. Marine Corps Base in Southern California; confirmed six UAS airspace entries between December 9–15, 2024.

Church Committee. The U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church (1975–1976). Cited as a precedent model for congressional accountability hearings preceding any future UAP disclosure.

CIA. Central Intelligence Agency. U.S. foreign intelligence service established 1947; convened the Robertson Panel in 1953, whose recommendations shaped seven decades of UAP information management.

CISA. Cybersecurity and Infrastructure Security Agency. Operational component of DHS established 2018 with responsibility for protecting U.S. critical infrastructure from cyber and physical threats.

Class A–D events. Tearsheet taxonomy of anomalous airspace event severity tiers used in the Crisis Playbook framing, from routine airspace anomaly (D) to multi-domain national-security event (A).

Clarke's Third Law. Arthur C. Clarke's aphorism that "any sufficiently advanced technology is indistinguishable from magic." Invoked in CU26 to underscore that the boundary between classified or advanced human technology and genuinely unexplained phenomena is not static.

Compartmentalization. The intelligence-community practice of restricting access to classified information by program-specific clearance ("special access program," SAP). Cited in CU26 in connection with classified UAP-relevant programs and disclosure governance.

Condon Report. *Scientific Study of Unidentified Flying Objects* (1968), authored by Edward U. Condon at the University of Colorado under USAF contract. Its conclusion that further study was unlikely to yield major scientific advances led to the closure of Project Blue Book in 1969.

CONOPS. Concept of Operations. A user-oriented description of how a system will be operated, used to derive engineering and integration requirements; recommend a CONOPS for spectral sensing on UAP-relevant aerial platforms.

Copenhagen Airport. Denmark's principal international airport; closed for nearly four hours on September 22, 2025 after multiple drone sightings, marking the opening of the European "Denmark" drone wave.

Counter-UAS. (C-UAS) Systems designed to detect, track, identify, and neutralize unauthorized unmanned aerial systems.

CRS. Congressional Research Service. Nonpartisan public-policy research arm of the U.S. Congress within the Library of Congress.

CU26. The inaugural edition of the Confronting Unknowns Program, conducted as part of the Massachusetts Institute of Technology's Independent Activities Period 2026.

CUF. Confronting Unknowns framework. The analytical pipeline proposed in this paper, organized as Detect → Identify → Respond → Explain (D-I-R-E), with explicit feedback loops between stages.

D-I-R-E. The four-stage Confronting Unknowns pipeline: Detect (capture and preserve evidence), Identify (translate evidence into ranked probabilistic hypotheses), Respond (decide and act under uncertainty), Explain (communicate to operational, legislative, and public audiences).

DARPA. Defense Advanced Research Projects Agency. The U.S. Department of Defense agency funding high-risk research in emerging technologies, established 1958.

Decision trap. A predictable cognitive failure mode under time pressure. The Crisis Playbook explicitly identifies four: premature closure, authority bias, availability bias, and anchoring.

Denmark drone wave. The September–November 2025 sequence of unidentified-drone incidents at Copenhagen, Aalborg, Kastrup, and other Danish, Norwegian, German, Belgian, and Dutch airports and military installations. Triggered Denmark's NATO consultations and the EU "drone wall" proposal.

DHS. Department of Homeland Security. U.S. federal department established 2002 with responsibility for domestic security, including critical-infrastructure protection, counter-UAS authority, and FEMA oversight.

DIAL. Differential Absorption LIDAR. Laser remote-sensing technique probing the atmosphere for specific chemical species, with potential application to ionization-trail and propulsion-byproduct detection.

Disclosure Act. See *UAPDA*.

Disinformation. The deliberate creation and dissemination of false information intended to mislead, as distinguished from misinformation (false but not deliberately so) and malinformation (true information shared maliciously out of context).

DoD. Department of Defense. The U.S. executive department overseeing the armed forces, intelligence components within those services, and acquisition activity, including UAP-related sensing assets and AARO.

DOE. Department of Energy. U.S. federal department with responsibilities including nuclear weapons stewardship; cited in the context of the "loose nuke" narrative around the New Jersey drone wave, which DOE and NNSA denied.

Doel nuclear power plant. Belgian nuclear generating station near Antwerp; five drones were reported circling the plant for roughly an hour during the November 2025 drone wave, prompting Belgium to request allied assistance.

DOJ. Department of Justice. U.S. federal executive department for law enforcement; holds primary federal counter-UAS authority alongside DHS.

Drone wall (EU). A European Union proposal, backed by EU leaders on October 1, 2025, to build a coordinated counter-drone perimeter along the eastern flank in response to the Denmark drone wave and Russian airspace violations.

DSCA. Defense Support of Civil Authorities. The DoD framework under which military forces support domestic civil authorities during emergencies (e.g., FEMA-led disaster response); referenced in ICS/NIMS scaling discussions.

EAR. Export Administration Regulations. U.S. Department of Commerce regulations controlling the export of dual-use goods, software, and technology. Cited alongside ITAR and the Atomic Energy Act as an export-control regime potentially applicable to UAP-derived technologies.

Earle. Naval Weapons Station Earle in Colts Neck, NJ; confirmed multiple UAS airspace entries on December 13, 2024.

Eastern Sentry. NATO mission launched September 2025 to reinforce the alliance's eastern flank after Russian drones violated Polish airspace and Russian MiG-31s entered Estonian airspace. Companion mission to Baltic Sentry.

Eindhoven Airport. Dutch civil-military airport in the southeastern Netherlands; suspended air traffic for several hours in November 2025 after multiple drone sightings, prompting the Netherlands to procure drone-detection radars.

Elsenborn. Belgian Army training-area and military base in the eastern cantons; site of drone sightings that opened Belgium's military-base wave in late October 2025.

EO. Electro-Optical. Sensors operating in the visible and near-infrared spectrum; includes standard cameras and telescope systems.

EO/IR. Electro-Optical / Infrared. Combined visible-band and infrared imaging sensor package; the standard fused payload on military targeting pods, surveillance aircraft, and counter-UAS platforms.

Erding. Bundeswehr air base near Munich, Germany; site of confirmed drone sightings on October 2–4, 2025, alongside operational disruption at Munich Airport.

Escalation ladder. A graduated sequence of community or institutional responses from passive observation through interception to neutralization. Included regarding the New Jersey case as a predictable consequence of an information vacuum.

F-22. F-22 Raptor air-superiority fighter operated by the U.S. Air Force, carrying the AN/APG-77 AESA radar. Used to shoot down the Chinese surveillance balloon in February 2023 and reportedly relocated during the December 2023 Langley incursions.

F-35. F-35 Lightning II multirole stealth fighter operated by the U.S. and allies, with a fused EO/IR sensor suite (DAS, EOTS); cited as being un-optimized for material identification despite advanced sensor integration.

F/A-18. F/A-18 Hornet and F/A-18E/F Super Hornet carrier-based multirole fighters operated by the U.S. Navy; carry the ATFLIR pod and AN/APG-79 radar that produced several widely circulated UAP videos.

FAA. Federal Aviation Administration. U.S. agency within the Department of Transportation responsible for civil aviation regulation, airspace management, and temporary flight restrictions (TFRs).

FBI. Federal Bureau of Investigation. U.S. domestic intelligence and law-enforcement agency within DOJ; opened public tiplines and coordinated investigative activity during the New Jersey drone wave.

FCC. Federal Communications Commission. Independent U.S. agency regulating interstate and international communications by radio, television, wire, satellite, and cable. Cited as one of the technology-risk-governance institutions relevant to anomalous-phenomena research and spectrum management.

FEMA. Federal Emergency Management Agency. Operational component of DHS responsible for federal disaster response, NIMS administration, and coordination with state emergency-management agencies.

Fifteen Minutes to Decide. Aspirational framing within the Crisis Playbook: a tool set for senior decision-makers facing an anomalous airspace incident within a fifteen-minute decision window, covering situation classification, contact protocols, decision-trap awareness, and graduated response options.

FLIR. Forward-Looking Infrared. A category of infrared imaging sensors mounted forward on aircraft and ground platforms for thermal imaging; also the company name (now Teledyne FLIR) producing many such systems including the Boson 640 LWIR core used by the Galileo Project.

FOCI. Foreign Ownership, Control, or Influence. The regulatory determination of whether foreign entities can direct or influence a U.S. company's decisions, triggering mitigation requirements before access to classified programs.

FOIA. Freedom of Information Act. U.S. federal statute (1966) providing public access to federal agency records subject to enumerated exemptions; the primary statutory tool for declassification requests on UAP-related material.

Galileo Project. Harvard-based scientific UAP research initiative led by Avi Loeb, operating multi-modal ground-based observatories with FLIR Boson LWIR arrays, passive multistatic radar, RF spectrum analyzers, and acoustic and geophysical sensors. Three observatories operational in MA, PA, and NV as of early 2026.

Gatwick incident. A December 19–21, 2018 closure of Gatwick Airport (UK's second-busiest) for roughly 36 hours due to repeated drone sightings; described by airport leadership as "highly targeted." A precedent for the airport-disruption pattern of subsequent waves.

Ge-68. Germanium-68, a radioactive isotope used in medical imaging calibration. A Ge-68 pin source lost in NJ-area transit on December 2, 2024 seeded the "loose nuke / dirty bomb search" theory of the drone wave; the source was subsequently recovered.

Geran-2. The Iranian-designed, Russian-produced Shahed-136 loitering munition under its Russian designation. Cited in the Russia–Ukraine war context that backgrounded European drone-wave attribution debates.

GIMBAL. One of the three U.S. Navy F/A-18 ATFLIR videos officially released by the DoD in 2020, showing an unidentified object exhibiting unusual rotation.

GNSS. Global Navigation Satellite System. The umbrella term for satellite-based positioning and timing systems including GPS (U.S.), GLONASS (Russia), Galileo (EU), and BeiDou (China); used for precision time synchronization in sensor networks.

GoFast. One of the three U.S. Navy F/A-18 ATFLIR videos officially released by the DoD in 2020, showing an unidentified object tracked at low altitude over the ocean.

GOES. Geostationary Operational Environmental Satellite. NOAA's geostationary satellite constellation providing continuous 16-band visible and infrared imaging of the Western Hemisphere at 5–15 minute cadence.

Gothenburg-Landvetter Airport. Sweden's second-busiest airport, on the country's west coast; observed one or more drones on November 6, 2025, forcing more than a dozen flights to reroute or cancel. Swedish police opened a "suspected aviation sabotage" investigation.

GPS. Global Positioning System. The U.S.-operated GNSS constellation providing geolocation and precise time; a frequent target of jamming and spoofing in contested environments.

Gremlin. An AARO sensor system developed by the Georgia Tech Research Institute, integrating long-range EO/IR cameras, 2D/3D radar, RF spectrum monitors, and ADS-B receivers. Tested March 2024 and deployed November 2024 to an undisclosed national-security site for 90-day baseline data collection.

H1. The first hypothesis: Data or Sensor Artifact. The apparent event is primarily a product of sensor behavior, processing error, or interpretation failure.

H2. The second hypothesis: Natural Physical Source. The event reflects a known atmospheric, astronomical, oceanic, or geophysical phenomenon (e.g., birds, ball lightning, meteors, mirage).

H3. The third hypothesis: Human-Made Physical Source (unclassified). The event reflects a real object consistent with conventional or commercially accessible technology (e.g., drone, balloon, satellite, crewed aircraft).

H4. The fourth hypothesis: Human-Made Physical Source (classified). The event reflects a real object associated with restricted state or defense activity, including allied or adversary test programs.

H5. The fifth hy: Unknown Physical Phenomenon. The event involves a real physical phenomenon not adequately explained by H1–H4. H5 functions as the hypothesis space's open residual: it holds probability for explanations the current set does not yet name, and is the category from which new, better-specified hypotheses are promoted as understanding develops. Probability should rest in H5 only after the artifact (H1), natural (H2), and human-technology (H3, H4) hypotheses have been seriously tested and found wanting, whereas H5 is a provisional holding place and not a default destination.

H1–H5. The five top-level explanatory hypotheses in the Confronting Unknown Framework's hypothesis space: H1 (artifact), H2 (natural), H3 (unclassified technology), H4 (classified technology), H5 (unknown). See individual H1, H2, H3, H4, H5 entries above.

H.654. Vermont House Bill H.654, introduced 2026 by Representative Troy Headrick. Would create a state airspace-safety and UAP task force to evaluate reports, assess risks, and coordinate scientific investigation.

HB 5422. Connecticut House Bill HB 5422, introduced 2026 by Representative Aundre Bumgardner. Would commission a state study of UAP in conjunction with law enforcement and state agencies to assess the feasibility of a state UAP center.

HR 8197. Federal bill introduced April 2026 by Representative Tim Burchett (R-TN). Would terminate AARO, redistribute its functions across existing Pentagon departments, and prohibit creation of any future centralized UAP office.

Human Observer. In the paper's credibility rating scale, one of five tiers from military-trained observer (rating 1) through untrained observer in poor conditions (rating 5), with hoaxer or confirmed-fabrication actors at rating 0.

Hynek classification. The 1972 civilian and academic system developed by J. Allen Hynek classifying UFO encounters as nocturnal lights, daylight discs, radar-visual, or close encounters of the first, second, and third kinds. Predecessor to modern operational taxonomies.

Hyperspectral imaging. Imaging that captures reflectance or emission across many narrow contiguous spectral bands, enabling identification of material classes (metals, polymers, composites) through their surface signatures. Typically operates from approximately 400 to 2,500 nm.

ICS. Incident Command System. The standard U.S. framework for organizing multi-agency emergency response, defining roles for command, operations, planning, logistics, finance, and public information. The paper argues that drone waves require clearer ICS triggers.

IGRA. Integrated Global Radiosonde Archive. NOAA archive of vertical atmospheric profiles from more than 2,800 stations worldwide, useful for correlating weather-balloon launches with UAP reports and assessing radar propagation anomalies.

Invention Secrecy Act. U.S. statute (1951) authorizing the federal government to impose secrecy orders on patent applications whose disclosure would be detrimental to national security. Cited in technology-governance discussion as one regime potentially applicable to UAP-derived discoveries.

IR. Infrared. Electromagnetic radiation with wavelengths longer than visible light. Subdivided into bands of increasing wavelength, VNIR, SWIR, MWIR, and LWIR, where different sensor technologies apply.

ISAR. Inverse Synthetic Aperture Radar. A radar imaging technique exploiting target motion to generate high-resolution shape and structural images, in contrast to SAR which exploits platform motion.

ISR. Intelligence, Surveillance, and Reconnaissance. Military operations and capabilities for gathering and analyzing information on adversary forces, activity, and environment.

ITAR. International Traffic in Arms Regulations. U.S. State Department regulations controlling the export and import of defense articles and services on the United States Munitions List. Cited alongside EAR and the Atomic Energy Act as an export-control regime applicable to potential breakthrough technologies.

JIC. Joint Information Center. The ICS-defined entity coordinating public information across agencies during a multi-jurisdiction incident; absent during the New Jersey drone response.

Kastrup. Kastrup Air Base in Denmark, a Royal Danish Air Force facility co-located with Copenhagen Airport; experienced drone sightings during the September 2025 wave.

Kinematics. The description of an object's motion (position, velocity, acceleration, heading) independent of the forces producing it; the sensor-derived motion record used to characterize candidate UAP events.

Kleine Brogel Air Base. Belgian Air Component base in Limburg; host facility for U.S. B61 tactical nuclear weapons under NATO nuclear sharing. Site of unidentified-drone activity for three consecutive nights in November 2025, which Defence Minister Theo Francken described as a deliberate spy operation.

Langley AFB. Joint Base Langley-Eustis, Virginia; home to the Air Force's first fighter wing. Experienced sustained nighttime UAS incursions over approximately 17 days in December 2023, prompting temporary relocation of F-22s to NAS Oceana.

LIDAR. Light Detection and Ranging. Active laser remote sensing providing high-resolution range, 3D geometry, and (in DIAL configurations) atmospheric chemical detection.

Likelihood. In Bayesian inference, the probability of the observed evidence given a particular hypothesis. Combined with the prior probability via Bayes' theorem to produce the posterior.

Liège Airport. Belgian cargo-and-passenger airport; repeatedly disrupted by drone sightings during the November 2025 Belgian drone wave alongside Brussels Airport.

LLM. Large Language Model. A class of AI models trained on large text corpora capable of natural-language understanding and generation; discussion on LLM-based normalization of heterogeneous UAP reports and uncertainty summarization.

LSST. Legacy Survey of Space and Time. The decade-long primary survey program of the Vera C. Rubin Observatory, imaging the entire visible sky every three nights across six optical bands; full operations expected 2026.

LWIR. Long-Wave Infrared. The 8–14 μm thermal-emission band; the primary band for passive thermal imaging independent of illumination.

Marche-en-Famenne. Belgian Army garrison in Wallonia; site of drone sightings investigated by Belgian authorities in late October 2025. Defence Minister Theo Francken stated the incidents were the work of skilled operators, not amateurs.

MECE. Mutually Exclusive and Collectively Exhaustive. A property of a hypothesis set in which categories do not overlap (mutually exclusive) and together cover all possibilities (collectively exhaustive). In the Confronting Unknowns Framework's hypothesis space, this property holds by construction: the fifth hypothesis (H5) is an open residual that absorbs any explanation the first four do not, so the set is exhaustive at every moment even though the explanations it names are expected to be revised, split, or added over time. Exhaustiveness is therefore a structural guarantee, not a claim that the named categories are final.

Micro-Doppler. Fine-grained modulations of a radar return produced by component motion (rotor blades, propeller, vibration). Used in modern counter-drone radar to discriminate between birds, rotary-wing drones, helicopters, and other low-RCS targets.

MiG-31. Mikoyan MiG-31 "Foxhound" Russian high-speed interceptor. Three MiG-31s violated Estonian airspace for approximately 12 minutes in September 2025, prompting Estonia's NATO Article 4 consultations.

ML. Machine Learning. Subset of artificial intelligence in which algorithms improve performance through exposure to data rather than explicit programming.

MM-LLM. Multimodal Large Language Model. An AI model integrating text with visual and other modalities, enabling reasoning over images, sensor plots, and structured data alongside natural language; central to CU26's AI-for-anomalies discussion.

MUFON. Mutual UFO Network. Civilian organization founded in 1969 maintaining a public database of more than 140,000 UFO/UAP case reports; the principal informal reporting channel through decades of federal disengagement.

Multipath. A radar artifact in which a signal reaches the receiver via more than one path (typically a direct return plus a ground- or surface-reflected return), producing apparent ghost targets. Listed as an H1 candidate.

Munich Airport. Germany's second-busiest airport (MUC); operations disrupted on two consecutive nights, October 2–4, 2025, after drone sightings, cancelling and diverting flights affecting thousands of passengers.

MWIR. Mid-Wave Infrared. The 3–5 μm spectral band; well suited to detecting hot engine components and exhaust plumes against cooler backgrounds.

NAS Oceana. Naval Air Station Oceana, Virginia; cited as the temporary relocation site for F-22s during the December 2023 Langley incursions.

NASA. National Aeronautics and Space Administration. U.S. civil space and aeronautics agency established 1958; administers ASRS for the FAA and commissioned the 2023 UAP Independent Study Team Report.

NEXRAD. Next-Generation Radar. A network of 160 S-band Doppler weather radars operated jointly by the NWS, FAA, and USAF, with publicly archived reflectivity, velocity, and spectrum-width products.

NIMS. National Incident Management System. The U.S. national framework, administered by FEMA, that standardizes preparedness and response across federal, state, tribal, and local agencies; ICS is one of its core components.

Nightcrawler. An electro-optical citizen-science detection system deployed by the Tedesco brothers off Long Island and during the New Jersey drone wave, sharing data with law enforcement and journalists; subject of academic publication and a 2025 *MIT Technology Review* feature.

Nimitz incident. A November 2004 series of encounters between U.S. Navy F/A-18s from the USS *Nimitz* carrier strike group and unidentified objects ("Tic Tacs") off the coast of Southern California; one of the canonical modern U.S. military UAP cases.

NIST. National Institute of Standards and Technology. U.S. Department of Commerce agency setting measurement standards and technology guidelines. Cited as among the technology-risk-governance institutions relevant to scientific investigation of anomalous phenomena.

NJDEP. New Jersey Department of Environmental Protection. Cited in connection with the "loose nuke" radioactive-material narrative that NJDEP and federal officials publicly refuted.

NNSA. National Nuclear Security Administration. Semi-autonomous DOE agency responsible for the U.S. nuclear weapons stockpile; denied the loose-nuke search theory of the New Jersey drone wave.

NOAA. National Oceanic and Atmospheric Administration. U.S. scientific and regulatory agency within the Department of Commerce operating the NWS, NEXRAD, GOES, and the IGRA archive.

NORAD. North American Aerospace Defense Command. U.S.–Canadian joint command responsible for aerospace warning, aerospace control, and maritime warning of North America. Tracked and shot down the February 2023 Chinese surveillance balloon and three additional unidentified objects.

NORTHCOM. U.S. Northern Command. The unified combatant command responsible for homeland defense of North America; cited in connection with radar and counter-drone reforms following Langley.

NRC. Nuclear Regulatory Commission. Independent U.S. federal agency regulating commercial nuclear power, materials, and waste; received the Palo Verde incursion reports and the December 2024 Ge-68 source-loss event report.

NSC. National Security Council. The White House body coordinating national-security policy across federal agencies. The paper's Tier 1 recommendation directs the NSC to develop and exercise inter-agency protocols for anomalous aerospace incursions.

NSF. National Science Foundation. Independent federal agency funding basic research and education across non-medical scientific disciplines; identified as a potential sponsor of a dedicated UAP research funding category.

NWS. National Weather Service. NOAA component operating U.S. weather observation and forecasting systems, including NEXRAD.

Observer Education Feedback Loop. The mechanism by which systematic public explanation of resolved UAP cases improves observer calibration, raising the signal-to-noise ratio of incoming reports and sharpening the residual unexplained set.

ODNI. Office of the Director of National Intelligence. U.S. office overseeing the 18-member Intelligence Community, established 2004; AARO and the predecessor UAPTF reported through ODNI channels.

OHSP. Office of Homeland Security and Preparedness (New Jersey). State-level homeland-security office that co-issued the December 2024 public tipline request with FBI Newark and the New Jersey State Police.

Palo Verde. Palo Verde Nuclear Generating Station, Arizona; experienced multiple unidentified UAV incursions on September 29–30, 2019, prompting an inter-agency investigation that closed without identifying operators.

PEMA. Pennsylvania Emergency Management Agency. State emergency-management agency whose director discussed UAP tracking at a February 2024 budget hearing referenced in CU26.

Phoenix Lights. A mass-witness UAP event on March 13, 1997, over Phoenix, Arizona, in which a large V-shaped formation of lights traversed the city; cited as a pre-social-media case that took weeks to reach national awareness.

Picatinny Arsenal. U.S. Army installation in Morris County, New Jersey, specializing in armaments R&D. Site of the November 13, 2024 opening incidents of the New Jersey drone wave.

Plant 42. Air Force Plant 42 in Palmdale, California, a government-owned advanced-aerospace facility associated with B-21 and other classified programs; experienced drone incursions on August 2–9, 2024.

Posterior probability. In Bayesian inference, the updated probability of a hypothesis after observing new evidence; the output of Bayes' theorem combining prior and likelihood. The hypothesis space H1–H5 ranking is a set of posteriors. Referred to in the main text as 'the updated probabilities' or 'the result.'

Premature closure. A decision trap in which an investigator declares a case resolved before evidence supports the conclusion ("it's just drones") in order to terminate analysis and public pressure. The defining failure mode in CU26's New Jersey case study.

Prior probability. In Bayesian inference, the probability assigned to a hypothesis before observing event-specific evidence. In UAP identification, priors reflect contextual factors such as proximity to military test ranges, atmospheric conditions, or known traffic patterns. Referred to in the main text in plain language as the 'starting assumptions' or 'starting probabilities.

Project Blue Book. U.S. Air Force program (1952–1969) that collected and analyzed more than 12,000 UFO reports under USAF's Air Technical Intelligence Center and successors; closed following the Condon Report.

Project Grudge. U.S. Air Force UFO investigation program (1949–1951), successor to Project Sign and predecessor to Project Blue Book; characterized by an explicit debunking orientation.

Project Sign. The first official U.S. Air Force UFO investigation program (1947–1949), prompted by the Kenneth Arnold sighting and the early postwar wave.

Project Galileo. See *Galileo Project*.

RAF Lakenheath. Royal Air Force base in Suffolk, England, hosting U.S. Air Forces in Europe (USAFE) units; experienced UAS incursions beginning November 20, 2024.

Ramstein. Ramstein Air Base in Germany, headquarters of USAFE; experienced unidentified-drone sightings in early December 2024.

RCS. Radar Cross-Section. A measure of how detectable an object is by radar, expressed in square meters and dependent on size, shape, and material. Modern counter-drone radars focus on the low-RCS regime where small, irregular targets dominate.

Remote ID. The FAA rule requiring most drones in U.S. airspace to broadcast identification and location information; recommendation is for fusing Remote ID with ADS-B, weather, and 911-call data in a universal operational picture.

RF. Radio Frequency. Electromagnetic spectrum used for communication and radar; RF emissions from unidentified objects are a key detection modality.

Robertson Panel. CIA-convened classified scientific review (January 1953) of UFO reports following the 1952 Washington, D.C. incidents. Its recommendation of a media and academic debunking campaign established the stigma architecture cited in Part III.

Roswell. The July 1947 recovery of unidentified debris near Roswell, New Mexico. The U.S. Army Air Field's initial "flying disc" press release was retracted the following day in favor of a weather-balloon explanation; the announce–retract–refuse pattern resembles a template for subsequent communication failures.

Rubin Observatory. See *LSST*.

SACEUR. Supreme Allied Commander Europe. NATO's senior military commander; referenced in alliance-level escalation discussions.

SAFER SKIES Act. 2025 federal legislation expanding the 2018 counter-UAS framework by allowing certified state and local officials to conduct approved counter-drone operations, creating a federal certification system and $250 million per year in funding for at least two years.

Safe Airspace for Americans Act. Proposed federal legislation addressing operational response authorities for anomalous airspace incursions.

SAR (radar). Synthetic Aperture Radar. Radar imaging that exploits platform motion to achieve high cross-range resolution; used in satellite-based maritime surveillance and terrain mapping. Distinct from ISAR.

Schiphol Airport. Amsterdam's principal international airport; closed one runway for 45 minutes in late September 2025 after a suspected-drone sighting during the Denmark drone wave.

SCU. Scientific Coalition for UAP Studies. U.S.-based nonprofit research organization convening academic and technical UAP work.

Sensor failure mode. A class of non-physical apparent detection produced by errors (hardware, calibration), artifacts (cosmic-ray hits, lens flare, compression), interference (weather, EMI, clutter), jamming, or spoofing. The CUF requires first-pass assessment against these modes for any anomalous detection.

SIGINT. Signals Intelligence. Intelligence derived from intercepted electronic signals and communications; "passive RF / SIGINT" is one of the sensor modalities surveyed in CU26.

Six observables. The set of characteristics used in U.S. policy discussions (including the UAP Disclosure Act) to identify UAP-like events: instantaneous acceleration absent apparent inertia; hypersonic velocity absent a thermal signature or sonic shockwave; transmedium travel; positive lift contrary to known aerodynamics; multispectral signature control; and physical or biological effects on close observers.

Skywatcher. A privately funded, active ground-based UAP observatory project launched in 2024, using high-zoom EO cameras, SWIR and MWIR imagers, radar, and passive RF/SIGINT sensors with multi-sensor kinematic fusion.

SNR. Signal-to-Noise Ratio. The ratio of signal strength to background noise; determines whether a sensor can reliably detect a given target.

Spoofing. Intentional deception of a sensor by injecting counterfeit signals (e.g., false GPS positions, false radar returns producing "ghost" targets). One of the sensor failure modes enumerated in CU26.

Stewart Airport. Stewart International Airport / Stewart Air National Guard Base, New York; closed for approximately one hour on December 13–14, 2024 after drone activity, with one UAS reportedly approaching within 25–50 feet of a C-17.

SWIR. Short-Wave Infrared. The 1–3 μm spectral band; used to detect reflected sunlight signatures and discriminate material classes including those carried by certain balloons.

Tic Tac. The colloquial name for the unidentified object encountered by U.S. Navy F/A-18s of the USS *Nimitz* strike group in November 2004 off Southern California, given for its smooth pill-like shape; one of the most studied modern military UAP cases.

Transmedium. Movement across distinct physical domains (e.g., air to water, space to atmosphere) without apparent transition. One of the six observables.

UAP. Unidentified Anomalous Phenomena. Current U.S. government designation, replacing the earlier "Unidentified Aerial Phenomena" usage. Covers events that cannot be immediately identified across air, sea, space, and transmedium domains.

UAP Assessment Matrix (Lomas). Five-dimensional credibility-rating framework for UAP evidence proposed by Lomas, O'Malley, Masters, and Vernet (2025, *Acta Astronautica* 234: 491–503). Cited in CU26 as a more detailed scientific-credibility scale than the operational five-tier observer rating used in the Detect section.

UAPDA. UAP Disclosure Act. Proposed U.S. legislation establishing formal declassification processes, an independent review board with eminent-domain authority over recovered materials, and mandatory reporting requirements for federal agencies and contractors.

UAPTF. UAP Task Force. The 2020 predecessor of AARO, established under the Office of Naval Intelligence to standardize collection and reporting on UAP encounters.

UAS. Unmanned Aircraft System. An unmanned aircraft (commonly called a drone) together with its ground control station and communications equipment.

UAV. Unmanned Aerial Vehicle. A powered aircraft without an onboard pilot, controlled remotely or autonomously.

UFO. Unidentified Flying Object. Legacy term for anomalous aerial sightings, replaced in U.S. policy usage by UAP since 2022.

UnHidden. UK-based nonprofit producing training materials for healthcare providers on supporting patients reporting extraordinary experiences; cited as having no current U.S. equivalent.

Unified Command. An ICS structure in which multiple agencies with jurisdictional authority share command of an incident while preserving their statutory roles; noted absence from the New Jersey drone response.

USAF. United States Air Force. Operated Project Blue Book (1952–1969) and currently operates NEXRAD radar stations jointly with NWS and FAA.

USAFE. United States Air Forces in Europe. The USAF major command headquartered at Ramstein; issued statements on the November 2024 incursions at RAF Lakenheath, Mildenhall, Feltwell, and Fairford.

USCG. United States Coast Guard. U.S. armed service operating under DHS in peacetime; provided observational reports of low-altitude aircraft near vessels during the December 2024 New Jersey drone wave.

UAP Independent Study. NASA-commissioned panel that issued its final report in September 2023, recommending (among other items) the expansion of ASRS to include systematic anomalous-event reporting by pilots and ATC.

Vandenberg SFB. Vandenberg Space Force Base, California; site of a November 30, 2024 incident in which a civilian (later identified as Chinese citizen and U.S. lawful permanent resident Yinpiao Zhou) was arrested for photographing the base by drone.

VASCO. Vanishing and Appearing Sources during a Century of Observations. Research project led by Beatriz Villarroel analyzing pre-Sputnik Palomar Observatory plates (1949–1957) for transient point sources; a 2025 *Scientific Reports* paper found transients clustered near nuclear-test dates and at rates consistent with sunlit objects in low Earth orbit.

VNIR. Visible and Near-Infrared. The 0.4–1.0 μm spectral band covering human-visible light and adjacent near-IR; the standard operating range of color cameras and most optical telescopes.

Volkel. Royal Netherlands Air Force base in the southeastern Netherlands; site where Dutch forces engaged drones with ground weapons in November 2025 without recovering the airframes.

Wright-Patterson AFB. U.S. Air Force base in Ohio; closed airspace for approximately four hours December 13–14, 2024 due to drone activity, with additional sightings on December 16–17.

Appendix B: Legislative Movements

Federal (enacted)

- **SAFER SKIES Act (2025):** Expands the 2018 federal counter-UAS framework by allowing certified local officials to conduct approved counter-drone operations, not just DOJ and DHS. It creates a federal certification and training system, potentially through FBI-approved courses, and fund the buildout with $250 million per year for at least two years.

Federal (proposed)

- **UAP Disclosure Act (UAPDA):** Would establish formal declassification processes, an independent review board with eminent-domain authority over recovered materials, and mandatory reporting requirements for federal agencies and contractors.
- **Safe Airspace for Americans Act:** Addresses operational response authorities for anomalous airspace incursions.
- **HR 8197** (introduced April 2026 by Representative Tim Burchett, R-TN): Would terminate the All-domain Anomaly Resolution Office, redistribute its investigative functions across existing Pentagon departments, and prohibit creation of any future centralized UAP office.

State (enacted)

- **New Jersey Assembly Bill A5712** (signed January 12, 2026, by Governor Phil Murphy as P.L. 2025, c.269): Establishes a Center for the Study of Unidentified Aerial Phenomena in partnership with a public institution of higher education, funded with $2.5 million in research grants. Total appropriation approximately $3.5 million including a related Air Traffic Controller Loan Redemption Program.

State (proposed)

- **Vermont House Bill H.654** (introduced 2026 session by Representative Troy Headrick): "An act relating to Vermont Airspace Safety and Unidentified Anomalous Phenomena Task Force." Would create a task force to evaluate UAP reports, assess airspace and public safety risks, and coordinate scientific investigation and reporting.
- **Connecticut House Bill HB 5422** (introduced 2026 session by Representative Aundre Bumgardner) "An act concerning a study of Unidentified Aerial Phenomena." Would undertake a study in conjunction with local law enforcement and state agencies of UAP by a scientific body in the state in order to assess the feasibility and benefits of establishing a state UAP center.

Appendix C: Existing surveillance, sensing, and reporting infrastructure

Table 12: Existing surveillance, sensing, and reporting infrastructures relevant to UAP analysis.

System	Data type	Relevance
NEXRAD Doppler Radar Network	160 S-band weather radars; reflectivity, velocity, spectrum width; publicly archived	Detects non-meteorological airborne returns; provides atmospheric baseline; nationwide continuous coverage enables retroactive analysis
GOES satellite constellation	16-band visible and IR imaging; full-disk every 5–15 minutes	Establishes environmental context concurrent with reported events; helps rule out meteorological explanations
Vera C. Rubin Observatory (LSST)	8.4 m survey telescope; six optical bands; entire visible sky every three nights; full operations expected 2026	Automated transient and anomaly alerts; AI/ML pipelines adaptable for anomalous-object detection in near-Earth or cislunar space
FlightRadar24 / OpenSky Network	ADS-B flight tracking; real-time and historical	Identifies cooperative air traffic near a reported event; objects in radar data absent from ADS-B may warrant investigation
MarineTraffic / AIS Networks	Global vessel tracking; real-time and historical	Rules out maritime vessel misidentification for coastal and over-water events
IGRA Radiosonde Archive	Vertical atmospheric profiles from 2,800+ stations globally	Identifies weather balloon launches correlatable with reports; atmospheric profiles help assess radar propagation anomalies
NASA ASRS	Confidential voluntary pilot and ATC safety reporting; 1.94 million cumulative reports over 47 years; approximately 100,000 per year	Recommended in the 2023 NASA UAP Independent Study [55] as a channel for systematic pilot UAP reporting within a trusted, destigmatized framework

Appendix D: Sensor Capabilities – Observables, Modalities, and Limitations

Characterizing an anomalous aerial object means asking two related questions: what do we want to learn about it? and which sensors can tell us? This appendix addresses both. The first part describes the six observable properties that distinguish one class of object from another; the second maps those properties onto specific sensor modalities, with their effective ranges and limitations. The detailed descriptions below expand on each observable property; and Table 13: Sensor capabilities and limitations at the end of this appendix translates them into hardware terms.

Observable Properties

Each observable answers a different question about a target. No single one is decisive on its own; their value comes from combination, since an explanation that satisfies one observable must also be consistent with the others.

Visual-Thermal Signature *(What it looks like)*: Describes the optical and thermal appearance of an object, including its shape, color, size, luminosity, and surface temperature. Electro-optical (EO) cameras operating in the visible band are the most common visual sensors. Infrared (IR) cameras, including forward-looking infrared (FLIR) systems, detect thermal radiation emitted by objects in wavelength bands invisible to the human eye, revealing whether a target is hotter or colder than its background (its thermal or heat signature). This can make thermally distinct objects detectable even when they are visually obscured, though an object at the same temperature as its surroundings may remain undetectable in IR as well. Combined EO/IR systems allow simultaneous visual and thermal observation.

Kinematics *(How it is moving)*: Describes the motion of an object: its position, altitude, velocity, acceleration, heading, and changes in direction. Radar is the primary kinematic sensor, measuring range, bearing, altitude, and radial velocity. LiDAR provides high-precision range measurement using laser pulses. GPS and multi-sensor tracking systems can fuse data to produce continuous three-dimensional flight paths. Kinematic data alone can be highly diagnostic: an object that hovers, reverses direction instantaneously, or sustains accelerations beyond known aerospace tolerances presents a signature that narrows the space of possible explanations. Note that kinematics describes *how* an object moves; inferring *why* it moves that way (the forces and energy involved) requires dynamic analysis, which is typically modelled from kinematic data rather than measured directly.

Propulsion Signatures *(What is driving it)*: Sensors can detect secondary indicators of an object's propulsion type, even when the propulsion system itself is not visible. FLIR can identify thermal exhaust plumes characteristic of chemical combustion (jet engines, rockets). Acoustic sensors detect sound generated by propulsion systems and aerodynamic surfaces, jet noise, propeller blade-pass frequencies, and rotor harmonics from helicopters and multirotor drones each produce distinctive acoustic signatures. The *absence* of expected propulsion signatures (e.g., an object maneuvering with no detectable thermal exhaust, acoustic emission, or aerodynamic control surfaces) is itself a significant observable.

Composition *(What it is made of)*: Describes the material makeup of an object. Hyperspectral imaging sensors measure reflected or emitted light across many narrow spectral bands, producing a spectral signature that can

distinguish broad material classes, metals, polymers, ceramics, vegetation, gases, by their characteristic reflectance or absorption features. This is distinct from elemental chemical analysis; hyperspectral sensors classify material types rather than identifying individual elements. Composition data is valuable for discriminating between target types (e.g., metallic aircraft vs. weather balloon vs. atmospheric plasma phenomenon such as ball lightning) when visual or kinematic data alone is ambiguous.

Radio-Frequency Emissions *(What signals it is transmitting)*: Detects active electronic transmissions from a target. Cooperative transponder systems, AIS (Automatic Identification System) for maritime vessels and ADS-B (Automatic Dependent Surveillance–Broadcast) for aircraft, broadcast identity, position, heading, and speed, from which registration and operator information can be queried through external databases. Electronic support measures (ESM) and wideband RF receivers detect non-cooperative emissions such as command-and-control (C2) links between drones and their operators, onboard radar, and telemetry downlinks. The *absence* of any detectable RF emission from an otherwise trackable object is itself a significant discriminant.

Magnetic Anomaly *(What disturbance it produces in the local field)*: Magnetometers detect deviations from the expected local geomagnetic field caused by ferromagnetic mass (e.g., an aircraft's metal structure), eddy currents induced by moving conductive bodies, or strong local electromagnetic sources. Magnetic anomaly detection (MAD) is an established technique in anti-submarine warfare and geological survey. In the context of UAP investigation, magnetic-field disturbances have been reported in proximity to unidentified targets, though the evidential basis for this correlation remains limited and the causal mechanism, if any, is not established [59].

Sensor Modalities and Limitations

The observables above are abstract; detecting them requires specific instruments, each with its own range, strengths, and blind spots. Table 13 below maps sensor modalities to the evidence they produce and notes, for each, whether it can resolve a representative discrimination problem, e.g., distinguishing a mylar balloon from a genuine unknown.

Table 13: Sensor capabilities and limitations

Sensor modality	Evidence type	Effective range	What it reveals	Resolves "balloon vs. unknown"?	Key limitation
Electro-optical camera (visible)	Dynamics	0.1–50 km	Shape, aspect ratio, angular velocity	Partial; short range only	No spectral, thermal, or compositional data
Infrared / FLIR	Thermal, dynamics	0.5–40 km	Thermal contrast; plume detection	Partial; emissivity unknown	Brightness temperature only; no absolute surface temperature without calibration
Radar (monostatic)	Dynamics	5–500 km	Track, RCS, ISAR imaging, Doppler velocity	No; mylar balloon approximates small metallic object in RCS	No material, no temperature; aliasing from scan rate
Passive RF / SIGINT	EM emissions	1–200 km	Frequency, modulation, power; fingerprints transmitter type	Partial; absence of emissions is a weak discriminator	Cannot detect non-emitting objects
Hyperspectral imager (VNIR/SWIR)	Composition	0.1–10 km	Surface reflectance spectrum identifies material class (metals, polymers, composites)	Yes; mylar has a sharp NIR absorption feature; metallic alloys do not	Requires good illumination (daylight); range limited by atmospheric scattering
Radiometry / pyrometry	Thermal	0.5–5 km	Detects anomalous thermal emission inconsistent with passive solar loading	Partial (requires companion sensor for emissivity)	Emissivity unknown for unidentified object; solar reflection contaminates MWIR
Laser LIDAR / DIAL	Composition, dynamics	1–5 km	High-resolution 3D geometry; DIAL probes atmosphere for ionization, ozone, or propulsion byproducts	Yes; resolves balloon shape, tether, and tumble	Requires active beam pointing; eye-safety constraints; not a wide-area search tool

Appendix E: Diagnostic Triage for Sensor Faults, Interference, and Deception

Before an anomalous-looking detection is treated as a genuine unknown, it must be assessed against the ordinary explanations that can mimic an anomaly. These fall into three broad families: a) faults internal to the sensor or its processing chain, b) effects imposed by the environment, and c) deliberate adversarial deception. Plus, there is a fourth case that is not an explanation at all: the residue that survives every check. This appendix first defines the categories, then operationalizes them into a triage table mapping each to its characteristic signature, the diagnostic questions that distinguish it, and the corresponding mitigations.

The five definitions below describe the mechanisms by which non-anomalous effects arise. Table 14 reorganizes the same material by operational family for use at the analyst's desk; the mapping is many-to-one rather than exact (for example, "Errors," "Artifacts," and "Interference" are distributed across the table's "Sensor and Pipeline" and "Environment and Propagation" rows), because the definitions are organized by cause while the triage table is organized by the workflow that rules each one out.

- Errors: faults in sensor hardware, calibration, or baselining. Examples: an uncooled thermal imaging sensor experiencing thermal drift that produces distorted object shapes; a radar altimeter with degraded calibration reporting incorrect target ranges.

- Artifacts: false signals generated by the sensing system itself during measurement or processing, which can cause non-physical phenomena to appear as real objects. Examples: cosmic ray hits on CCD/CMOS sensors producing bright pixel anomalies that can be mistaken for point-source objects; lens flare or internal reflections (glare) creating apparent objects in optical and infrared imagery; digital compression or processing artifacts distorting object shape or motion. Aperture-shape artifacts, in which point sources photographed out of focus take on the geometric shape of the lens aperture (often triangular, hexagonal, or octagonal), are a documented source of apparent "structured craft" in civilian footage [60].

- Interference: environmental factors that degrade sensor accuracy. Examples: adverse weather conditions (rain, fog, humidity) reducing optical and infrared sensor performance; electromagnetic interference from solar activity affecting RF sensors; physical clutter in the sensing environment such as birds, debris, or airborne particulates generating false returns.

- Jamming: the intentional emission of RF energy to overwhelm or deny legitimate sensor signals, resulting in degraded detection capability. Examples: GPS or communications jamming in conflict zones. Jamming can make detection and tracking of anomalous objects significantly more difficult in contested electromagnetic environments.

- Spoofing: intentional deception of sensors to cause them to report false data. Examples: broadcasting counterfeit GPS signals to cause receivers to report false locations, altitudes, or speeds; electronic warfare techniques that inject false radar returns, producing "ghost" targets that can make objects appear to perform impossible maneuvers such as instantaneous acceleration or rapid directional changes.

Table 14: Diagnostic triage for characteristic signatures, investigative questions, and mitigations for the principal classes of explainable effect that can masquerade as an anomalous detection, plus the residual case of a genuine unresolved signature.

Failure mode	Typical "anomalous" signature	Investigative questions	Mitigations
Sensor and pipeline error			
Calibration drift or bias	Persistent offset in range, angle, or velocity; "impossible" kinematics	Was calibration verified post-sortie? Does bias correlate with temperature or time-on?	Calibration checks; environmental compensation; health monitoring
Time-synchronization error	Tracks that "jump"; inconsistent fusion; false acceleration	Are clocks GNSS-disciplined? What is the time-base error bound?	Clock discipline; timestamp provenance; sync alarms
Resolution, aliasing, thresholding	Object flickers at detection threshold; track fragmentation	Is SNR near threshold? Any changes in gain or filters?	Record raw data; adaptive threshold; confidence scoring
Multipath, sidelobes, clutter	False targets, mirrored trajectories, sudden bearing changes	Is geometry conducive to multipath? Are sidelobe-suppression settings known?	Site characterization; sidelobe controls; independent geometry cross-check
Environment and propagation			
Atmospheric ducting or refraction	Radar range and bearing distortions; "over-the-horizon" surprises	Are meteorological conditions consistent with ducting?	Integrate meteorological and ocean models; annotate propagation regime
Geophysical interference	Magnetometer or EO artefacts; spurious signals in specific regions or times	Are there known geomagnetic or solar-activity factors?	Fuse space-weather context; flag elevated uncertainty regimes

Deception and information warfare			
Spoofing	Consistent but false tracks; alignment with adversary operational objectives	Do signals show protocol inconsistencies? Correlation with known EW patterns?	Cryptographic and authenticated ranging; anomaly detection; independent sensor cross-checks
Jamming	"Nothing seen" by one sensor; detection gaps; noisy bands	Is there spectral evidence of interference?	Spectrum monitoring; multi-band diversification; fallback procedures
Genuine unresolved signature			
Cross-modal inconsistency without plausible artefact	Multiple independent modalities disagree in ways that do not map to known artefacts	Do independent sensors share common failure modes? Is there raw-data retention?	Escalate with structured uncertainty; preserve data; attempt controlled re-observation

Appendix F: Current UAP observatory projects

Dedicated UAP observatories, such as Harvard's Galileo Project, can complement incidental detections by improving calibration and synchronization while producing gold-standard datasets that fill the gap of existing sensor systems designed for other purposes. Such efforts can be a complement to historical surveys of astronomical data, like the VASCO project (see e.g. [61], [62]).

Table 15: Current UAP observatory projects

Project and Type	Description	Sensors involved
Galileo Project [53] Ground-based observatory (passive)	Host: Harvard University. Established: 2024. Funding: Foundation grant. Description: 3 observatories operational in MA, PA, NV as of early 2026; 4th planned in IN.	Wide-field multispectral cameras (eight FLIR Boson 640 LWIR in all-sky array); narrow-field optical instruments (imaging, spectroscopy, polarimetry, photometry); passive multistatic radar; radio spectrum analyzers; acoustic sensors (infrasonic to ultrasonic); environmental sensors; geophysical sensors; energetic particle detectors
AARO Gremlin system [63] Ground-based observatory (government + academic)	Host: Georgia Tech Research Institute for AARO. Established: 2024. Description: tested March 2024; deployed to undisclosed national security site November 2024 for 90-day baseline collection)	Long-range electro-optical cameras; infrared sensors; 2D search radar; 3D radar; RF spectrum monitors; ADS-B transponder receivers
UAPx Inc. [64] Ground-based field observatory (passive)	Affiliation: University at Albany. Established: 2021. Description: Non-profit. Using visual, infrared, and radiological measurement devices.	Visible-light cameras; infrared cameras; night-vision optics; radiation detectors; cosmic-ray and high-energy particle detectors; multi-sensor optical tracking units; external corroboration via weather radar and satellite imagery
Skywatcher [65] Ground-based observatory (active)	Independent initiative focused on aerial intelligence, advanced sensing, and unconventional aerospace research.	Electro-optical cameras (high-zoom visible); infrared imagers (SWIR and MWIR); radar; passive RF receivers and spectrum analyzers; telemetry and SIGINT sensors; kinematic tracking via multi-sensor fusion

Appendix G: “Drone Wave” Timelines

This appendix compiles open-source reporting on the unexplained drone and uncrewed-aircraft incidents that drove aerospace airspace anxiety from 2014 through early 2026, organized to show how scattered incursions hardened into two large, politically consequential "waves."

It runs in four movements. Precursors (2014–2024) establish that incursions over nuclear sites, airports, and military installations recurred on both sides of the Atlantic well before they drew sustained attention. The American Northeast ("NJ") wave of late 2024–early 2025, together with the concurrent military-installation reports beyond the Northeast, marks the pattern reaching critical mass in the United States. The European ("Denmark") wave of fall 2025, unfolding against the Russia–Ukraine war, shows a similar dynamic across NATO airspace under geopolitical pressure. A closing set of recurrences confirms the phenomenon receded rather than resolved.

Entries vary widely in evidentiary weight, from confirmed installation statements and recovered records to single-witness reports and official briefings later qualified or contradicted. Inclusion is not an endorsement of any one explanation, mundane or adversarial. Read against the four-failure analysis in Part III, that variance is the point: it shows how thin, conflicting signals were repeatedly forced into premature narratives, and where the detect-to-decide chain bent or broke.

Precursor incidents before the 2024–2025 NJ and Denmark-centered drone waves

U.S. precursor incidents

September 29-30, 2019 - Palo Verde nuclear-plant incursions

> Multiple UAVs were reported over the Palo Verde Nuclear Generating Station. Site security could not identify markings on the aircraft or locate the operators, and plant officials coordinated with NRC personnel, local law enforcement, the FBI, DHS, and FAA; an FBI weapons-of-mass-destruction coordinator was also contacted, ending with an inconclusive investigation. [66]

December 2019-January 2020 - Nebraska-Colorado mystery-drone wave

> Credible witnesses, including law enforcement personnel, reported formations of sizable aerial devices (up to 6-foot wingspans) across Nebraska and Colorado. The FAA launched an investigation, with records later indicating that officials could not determine the origin of the devices. They expressed “high confidence” that they were not covert military activity and noted no (released) evidence of federal criminal violations or military-installation incursions. [67], [68]

February 1-12, 2023 - Chinese surveillance balloon and NORAD shootdowns

> A Chinese high-altitude surveillance balloon was publicly acknowledged over Montana on February 1, 2023; an F-22 downed it off the coast of South Carolina on February 4 after a week-long transit of the continental United States. NORAD then adjusted radar filter parameters and, over the following week,

detected three additional unidentified objects, which were shot down over Deadhorse, Alaska (February 10), Yukon, Canada (February 11), and Lake Huron (February 12). Three of the four were never positively identified, and debris recovery was incomplete or impossible. The sequence prompted the cancellation of Secretary Blinken's planned Beijing visit and remains the highest primary-source-density U.S. air-defense intruder case of the period, a doctrinal precursor that made later airspace intruders more visible while leaving the detect-to-decide chain visibly fragile. [69]

December 2023 - Langley Air Force Base precedent

CBS reported that drones appeared over Langley Air Force Base for 17 nights, with objects arriving after sunset and ranging from commercial quadcopters to larger craft. Retired Gen. Glen VanHerck described a response involving fighters, AWACS platforms, and helicopters, while emphasizing that homeland radar and legal authorities were poorly adapted to low-flying drone activity; some F-22s were reportedly relocated and later NORTHCOM reforms focused on more sensitive radar and deployable counter-drone kits. [70]

August 2-9, 2024 - Plant 42 incursions

Air Force Plant 42 in Palmdale, California, a major advanced aerospace-development hub, experienced a series of reported drone incursions. Temporary flight restrictions were later imposed on August 14 around the local airport, and FOIA-based reporting identified specific incursions between August 2 and August 9, raising concern because the facility supports highly sensitive military programs. [71], [72]

European precursor incidents

October-November 2014 - French nuclear-site overflights

Unidentified drones were reported over multiple French nuclear facilities. France's Secretariat-General for National Defense and Security characterized the flights as an "organized provocation" geared towards "disrupting the chain of surveillance and protection at these sites", while the environment minister said officials did not have a lead on who was operating them. [73]

December 19-21 2018 - Gatwick Airport disruption

Drones reportedly shut down Gatwick, the United Kingdom's second-busiest airport, for roughly 36 hours. Gatwick CEO Stewart Wingate, in a December 20, 2018 statement, described the flights as "highly targeted" and "designed to ... bring maximize disruption". At points, aircraft were left to circle the airport, running low on fuel. The military deployed an anti-drone system to the airport. [74]

January 2022 - Swedish nuclear-plant sightings

Swedish authorities investigated drone reports at the Forsmark, Oskarshamn, and Ringhals nuclear plants, leading to police deployment of helicopters and additional national security investigations. The aircraft were described as capable of operating in high winds, and the episode occurred amid additional reports near government buildings. [75], [76]

May 14, 2023 - Gatwick runway closure

Gatwick temporarily closed its runway for almost an hour after a suspected drone sighting near the airfield. Twelve incoming flights were diverted while the airport followed established procedures and investigated the report. [77]

American Northeast "NJ" drone timeline: late 2024–early 2025

November 13, 2024 - Picatinny Arsenal opening incidents

Picatinny Arsenal personnel begin to observe lights of unknown origin maneuvering above the military installation, which is close to residential areas. This made the early New Jersey wave more than a residential sighting cluster, because a sensitive military site was involved at the outset. [7]

Around November 18, 2024 - Morris County reports multiply

Reports began multiplying around Morris County and northern New Jersey. Reuters reported that the FAA began receiving reports from Morris County around November 18, while federal officials investigated with state and local partners and cautioned that some sightings could involve manned aircraft or inaccurate reports. [78]

November 22, 2024 - FAA restrictions begin

The FAA prohibited drone flights over Trump National Golf Club in Bedminster after unexplained drone activity, later extended on November 25 to Picatinny Arsenal, after reports of unexplained drone activity. [79]

November 26, 2024 - Raritan Valley medevac disruption

A reported drone sighting near Raritan Valley Community College diverted a medevac helicopter from its planned landing zone; the patient was successfully transported via a secondary landing zone at Somerset Airport in Bedminster. Later reporting on federal documents suggested the case may have involved misidentified aircraft near Solberg Airport, making it important as an example of how even mistaken reports amid a drone wave can create real emergency-response consequences. [80]

December 3, 2024 - FBI public tipline opens

FBI Newark, the New Jersey State Police, and the New Jersey Office of Homeland Security and Preparedness asked the public to report information related to recent possible drone sightings along the Raritan River. The FBI said reports from the public and law enforcement dated back several weeks and included clusters resembling drones and a possible fixed-wing aircraft. [81]

Commentary: Institutional resistance to outside expertise

Rolling Stone reported that Craig Robertson, a retired Army major and counter-UAS specialist, offered assistance to New Jersey State Police and the FBI; his attempts to push deeper went cold. The pattern illustrates a recurring theme: institutions with operational gaps declined external expertise rather than admitting the gap existed. (See *Part III: Respond & Explain* and [8].)

December 8, 2024 - Morris County mayors escalate

Pequannock Mayor Ryan Herd circulated a letter to Governor Phil Murphy that was signed by 21 Morris County mayors within days. The letter said local efforts had been hindered by a lack of information and called the situation untenable. [82]

December 10, 2024 - State emergency-operations briefing

News 12 reported that mayors left a New Jersey drone-sightings briefing frustrated, with Herd saying officials still did not know who was responsible or where the drones were coming from. Rolling Stone later reported Herd's recollection that roughly 185 mayors attended the Ewing briefing, which included senior representatives from the New Jersey State Police, FBI, DHS, and DoD. [8], [83]

December 10-11, 2024 - Coast Guard vessel report

A Coast Guard Lieutenant told AP that "multiple low-altitude aircraft were observed near one of our vessels near Island Beach State Park". Middletown mayor Tony Perry claimed up to 40 drones were spotted, some at speeds of 60-70 mph. Rep. Chris Smith separately amplified claims that 12 to 30 drones followed a Coast Guard lifeboat. [84], [85]

December 11, 2024 - Legislator briefing details circulate

Briefing notes and public reporting described drones as up to six feet wide, able to operate for six to seven hours, sometimes with lights off, and allegedly able to avoid ordinary detection. [84]

December 10-11, 2024 - Adversary theories enter politics

Rep. Jeff Van Drew claimed that a trusted source told him an Iranian ship offshore was launching drones and called for them to be shot down. The Pentagon directly denied the claim, with Reuters reporting there was no Iranian drone mothership off the United States and no evidence the drones were coming from a foreign entity or adversary. [85]

December 12, 2024 - DHS/FBI and White House say no known threat

DHS and the FBI issued a joint statement saying they had no evidence at the time that the reported sightings posed a national-security or public-safety threat or had a foreign nexus. They also said they were working to determine whether the reports involved drones, manned aircraft, or inaccurate sightings. White House spokesperson John Kirby made similar statements. [1], [78]

December 12–13, 2024 - Drones reported near Salem/Hope Creek nuclear plant complex

Utility company PSE&G reported drone activity near the Salem and Hope Creek nuclear complex in Salem County and said it had contacted federal authorities. The utility asked the FAA to restrict airspace over the site, while Rep. Jeff Van Drew publicly cited reports of drones near the facility and called for stronger federal action. [86]

December 13, 2024 - Naval Weapons Station Earle confirms entries

Naval Weapons Station Earle in Colts Neck, NJ confirmed multiple instances of unidentified drones entering its airspace. The base said no direct threat had been identified. [87]

December 13-14, 2024 - Stewart Airport runway closure

New York Governor Kathy Hochul stated that the runways at Stewart Airfield were shut down for approximately one hour because of drone activity. Rep. Pat Ryan said the UAS got within 25-50 feet of a C-17 military transport plane. [88], [89]

December 14-15, 2024 - Boston Logan-area arrests

Boston police arrested two men after a hazardous drone operation near Logan Airport airspace from Long Island in Boston Harbor. The case appears to be an ordinary illegal-drone enforcement matter rather than an unexplained base incursion, occurring during the broader Northeast wave. [90]

December 14-16, 2024 - Federal detection finds little wrongdoing

AP reported that drone detectors deployed in New Jersey found little or no evidence of wrongdoing. Governor Murphy said only a limited number of suspected sightings had been reported over the weekend, while federal officials continued saying they had no indication of foreign involvement or harmful intent. [91]

Mid-December 2024 - Lasers and firearms become hazards

The FAA warned of a spike in people pointing lasers at aircraft during the wave, while the FBI warned the public not to shoot at suspected drones. [92]

December 15, 2024 - Schumer seeks drone-detection tools

Sen. Chuck Schumer urged DHS to deploy state-of-the-art drone-detection technology across New York and New Jersey. He also said he would co-sponsor legislation giving local authorities more drone-detection tools. [93]

December 16-17, 2024 - Multi-agency statement quantifies public tips

DHS, FBI, FAA, and DoD said the FBI had received more than 5,000 tips, generating roughly 100 leads. The agencies assessed the reports as a mix of lawful commercial drones, hobbyist drones, law-enforcement drones, manned aircraft, helicopters, and stars, while saying unauthorized activity over restricted military airspace was being taken seriously. [94]

December 15-16, 2024 - Mayorkas calls for expanded authorities

DHS Secretary Alejandro Mayorkas said there was no known foreign involvement in the mass drone sightings. At the same time, he called for Congress to expand federal counter-drone authorities. [95]

December 17, 2024 - Biden says no sense of danger

President Biden said federal officials were following the sightings closely but had no sense of danger. Mayorkas separately said the federal government had deployed additional personnel, resources, and technology to assist New Jersey State Police. [96]

Mid-December 2024 - Missing-radioactive-material theory denied

The NRC event report stated that a Ge-68 pin source lost in transit on December 2 had been found, returned to the supplier, and closed as an incident involving material less than Category 3. NJDEP and federal officials later said the theory that drones were tracking missing radioactive material was false and that drones were not used to search for it. [97], [98]

December 18-19, 2024 - FAA expands critical-infrastructure restrictions

The FAA imposed temporary 30-day drone restrictions over 22 critical-infrastructure locations in New Jersey after requests from federal security agencies. The affected areas included Jersey City, Elizabeth, and Camden, while New York also moved to restrict drone flights over critical-infrastructure sites. [92]

December 19, 2024 - Counter-UAS authority becomes flashpoint

AP reported that federal authority to track and disable threatening drones was becoming entangled in budget negotiations and nearing expiration. [99]

Mid-late January 2025 - Temporary FAA restrictions expire

The December FAA restrictions were generally framed as one-month measures extending into mid-January. Their expiration marked the administrative wind-down of many emergency restrictions imposed during the height of the New Jersey wave.

January 28, 2025 - White House closure statement

Press Secretary Karoline Leavitt stated that the drones seen over New Jersey had been authorized by the FAA for research and other purposes and that many also involved hobbyist or recreational activity. No further explanation has emerged since. [100]

Concurrent military reports beyond the U.S. Northeast

November 20-26, 2024 - U.S. bases in the United Kingdom

The U.S. Air Force said small UAS continued to be spotted near and over RAF Lakenheath, RAF Mildenhall, RAF Feltwell, and RAF Fairford beginning November 20, with fluctuating numbers and varied sizes and configurations. Reuters reported a U.S. official saying the drones did not appear to be hobbyist activity and seemed coordinated, while parliamentary proceedings reflected local public concern about aircraft being scrambled at night; a later written answer said the incidents remained under active investigation as of June 2025. [101], [102], [103], [104]

November 30, 2024 - Vandenberg Space Force Base overflight and later arrest

DOJ announced that a 39-year-old Chinese citizen and U.S. lawful permanent resident, was arrested at San Francisco International Airport en route to China for allegedly flying a drone over and photographing Vandenberg Space Force Base. [105]

December 3-4 2024 - Ramstein Air Base sightings

Unidentified drones were spotted over Ramstein Air Base in Germany in early December, with confirmation from a U.S. Air Force spokesperson. [106]

December 9-15, 2024 - Camp Pendleton incursions

Marine Corps Base Camp Pendleton confirmed six instances of unmanned aerial systems entering its airspace. The base said there was no threat to installation operations. [107]

December 13-17, 2024 - Wright-Patterson airspace closures

Drones around Wright-Patterson Air Force Base forced officials to close base airspace for roughly four hours on December 13-14. The base later reported additional small UAS overnight on December 16-17, with fluctuating numbers and varied sizes but no effect on residents, facilities, or assets. [108], [109]

December 2024 - Hill Air Force Base sightings

Hill AFB confirmed that unmanned aerial systems had been spotted near the base in Davis County, Utah. Officials said they were monitoring the area and working with local authorities. [110]

December 17-19, 2024 - Fort Worth-area suspicious activity

White Settlement police reported suspicious drone activity near military and federal sites, including areas near Naval Air Station Joint Reserve Base Fort Worth, a Lockheed Martin facility, and a Texas Army National Guard recruitment center. Police coordinated with security personnel and later worked with the FBI, NCIS, and the Air Force. [111]

December 2024–January 2025 - Bavarian military-base sightings

Bavaria's State Office of Criminal Investigation investigated suspected Russian espionage after drones were spotted over several Bavarian military installations, including the Manching facility and a military site at Neuburg an der Donau. The Manching base had sightings on multiple days in December, with another incident reported in January. [112]

Commentary: Scale context from NORAD testimony

In February 2025 Senate Armed Services testimony, Gen. Gregory Guillot stated that there were 350 UAS detections over 100 different U.S. military installations in 2024. The testimony placed the late-2024 cases into a broader military-installation security problem. [113]

European “Denmark” drone wave timeline

Denmark wave: September–November 2025

September 22-23, 2025 - Copenhagen and Oslo airport closures

Two or three large drones were reported near Copenhagen Airport, closing it for nearly four hours, while Oslo Airport also shut its airspace for about three hours after a drone observation. Danish police reportedly described the Copenhagen drones as likely operated by a capable operator based on size, number, flight pattern, and behavior; Norway later ended the Oslo probe for lack of evidence. [114], [115]

September 24-27, 2025 - Danish airports and military sites

Drones were reported at Kastrup Air Base, as well as airports with military roles Aalborg, Esbjerg, Sønderborg, Skrydstrup, and Billund. This caused disruptions, diversions, and additional closures. Denmark told NATO allies unspecified state actors were responsible even as Danish officials publicly said attribution remained unclear; Danish Defence confirmed drones at several facilities and said several capabilities were deployed. Danish emergency response moved to operational readiness after additional suspicious activity and police received more than 500 drone-related reports nationally in 24 hours. [116], [117], [118]

September 25-October 1, 2025 - Northern Germany critical-infrastructure reports

German authorities investigated unidentified drones over critical infrastructure in Schleswig-Holstein, including a power plant, a university hospital, a shipyard and defense-industrial area in Kiel, and a military base in Sanitz in a nearby state. [119]

September 27, 2025 - Amsterdam airport runway closure

Amsterdam’s Schiphol Airport closed a runway for 45 minutes after a sighting of a suspected drone. [120]

September 27-28, 2025 - Denmark bans civilian drone flights

Denmark ordered a week-long ban on civil drone flights after fresh sightings at military facilities. The Danish military said it had deployed several capacities in response to overnight sightings, while declining to describe the response in detail. [121]

September 27-28, 2025 - Norwegian airbase and airport reports

Norwegian police investigated possible drone sightings near Ørland air base, Norway’s main F-35 base, after guards reported several observations outside the perimeter. Additional reporting described flight disruptions linked to drone reports near Bardufoss and Brønnøysund airports. [122], [123], [124]

September 28, 2025 - Finland hydroelectric-plant report

A passerby reported an unidentified drone over the Valajaskosken hydroelectric power plant in Rovaniemi, Finland. Regional law enforcement confirmed the report but withheld details because of

investigative measures. The incident happened recently after Finnish power plants became no-fly zones. [124], [125]

October 2-4, 2025 - Munich Airport and Erding base disruption

Munich Airport operations were affected two nights in a row after drone sightings, canceling and diverting flights affecting thousands of passengers. Germany's defence ministry confirmed media reports that drones were spotted over a nearby ammunition depot and the Erding military base. [126]

October 8, 2025 - Germany broadens police powers

Germany moved to give police broader authority to shoot down drones. [127]

October 2025 - Belgian military-base sightings

Belgium opened an investigation after drone sightings over military bases including Marche-en-Famenne and Elsenborn. Defence Minister Theo Francken said the incidents were not the work of amateurs but of skilled drone pilots. [128]

October 31-November 2, 2025 - Berlin and Bremen airport suspensions

Berlin Brandenburg Airport suspended flights for nearly two hours after a late-evening drone sighting, and police confirmed a witness report but did not find the drone. Bremen Airport also temporarily suspended takeoffs and landings after a drone was spotted nearby, with at least one flight diverted and another delayed. [129], [130], [131]

November 1-9, 2025 - Belgian airports, bases, and nuclear plant

Unidentified drones were reported over Kleine Brogel Air Base, host to U.S. B61 tactical nuclear weapons under NATO nuclear-sharing, for three consecutive nights, and Defence Minister Theo Francken called the activity a deliberate spy operation: "small drones probing radio frequencies, then larger drones to destabilize," not amateur activity. Chief of Defence Admiral Frederik Vansina ordered the military to shoot down unidentified drones over Belgian military bases. Brussels and Liège airports were repeatedly shut down after drone sightings, with more than 50 Brussels flights canceled on November 4 and roughly 500 passengers spending the night in the terminal; five drones were later reported circling the Doel nuclear power plant for about an hour. Belgium subsequently brought in allied armed forces to help track or seize drones around airports, military bases, and the nuclear plant. Later reporting suggested an incursion over the port of Antwerp. [132], [133], [134], [135], [136]

November 6, 2025 - Sweden's Gothenburg airport disruption

One or more drones were observed at Gothenburg-Landvetter Airport on Sweden's west coast, forcing more than a dozen flights to be rerouted or canceled. Swedish police opened an investigation into "suspected aviation sabotage". [137]

November 21-22, 2025 - Dutch military fires on drones

The Dutch military used ground weapons against drones spotted above Volkel air base in the southeastern Netherlands, but the drones left and were not recovered. Eindhoven Airport, which serves both civilian and military functions, suspended air traffic for several hours because of multiple drone sightings, and the Netherlands later moved to buy drone-detection radars. [138], [139], [140]

Mid November-early December 2025 - French military-installation overflights

From November 10-12, incursions over Eurenco munitions facility in Bergerac, and a separate incursion over a train in Mulhouse carrying tanks, led to a mobilization of the French national police. From November 26-30, suspected drones appeared at Base Aerienne de Creil, including up to six hostile drones over three nights at a base housing military intelligence and satellite-monitoring functions. In early December, several unidentified drones were reported to fly over France's Ile Longue strategic nuclear-submarine base, where technical means detected them and marines deployed countermeasures, public prosecutor Frédéric Teillet later clarified that the response involved a jammer, not firearm fire. Additional incursions were previously reported nearby on the Crozon peninsula in November. [141], [142], [143], [144]

Context alongside the Russia–Ukraine war

January 2025 - NATO launches Baltic Sentry

NATO launched Baltic Sentry to protect undersea cables, telecom links, and pipelines in the Baltic Sea after incidents involving damaged seabed infrastructure. The mission would involve frigates, patrol aircraft, naval drones, better surveillance, and closer private-sector coordination. [145]

September 10-12, 2025 - Russian drones enter Polish airspace

Poland shot down Russian drones that violated its airspace during Russia's war against Ukraine, an action Reuters described as the first known case of its kind by a NATO member during the war. NATO then launched Eastern Sentry to reinforce the eastern flank after Russian drones violated Polish airspace. [146]

September 13, 2025 - Romanian airspace Shahed incursion

Romania became the second NATO state penetrated in the September 2025 wave when a Russian Geran-2 (Shahed-136) drone violated its airspace from Ukrainian territory. Romanian Air Force F-16s tracked the drone for roughly 50 minutes; the pilots had authorization to engage but withheld fire because of the risk to populated areas on the ground. The Romanian Ministry of National Defence issued a same-day statement confirming the incursion and the engagement decision. [147]

September 19-23, 2025 - Russian jets violate Estonian airspace

Estonia said three Russian MiG-31 fighter jets violated its airspace for around 12 minutes; Russia denied the claim. NATO said allied aircraft intercepted and escorted the jets out, prompting Estonia to request Article 4 consultations. [148]

October 1, 2025 - EU leaders back a 'drone wall'

In the middle of the drone wave, EU leaders backed creation of a drone wall as a countermeasure against Russia. [149]

Selected post-wave recurrence incidents

March 2026 - Barksdale Air Force Base recurrence

Air Force Global Strike Command stated that Barksdale AFB experienced several unauthorized drone incursions beginning March 9, 2026, with varying duration and numbers of drones. The base issued and then lifted a temporary shelter-in-place order, continued operations, and said a federal investigation remained active. [11]

March 11, 2026 - Berlin airport suspension

Berlin Brandenburg Airport (BER) briefly suspended takeoffs and landings after an unknown object was reported near a Bundeswehr (German military) helicopter hangar. Operations were paused for roughly half an hour as a safety precaution. [150]

Appendix H: Simple Probabilistic Case Analysis

Bayesian reasoning is a method for reasoning under uncertainty. It states plainly what is believed before new evidence arrives, revises that belief as evidence comes in, and produces a range of possibilities each weighted by how likely it is, rather than a single verdict. For policymakers, the appeal is practical: it requires analysts to put their assumptions in writing, makes any disagreement easy to trace to its source, and allows an assessment to be updated as new facts emerge.

We apply here a simple probabilistic model to a toy example. See the following sources for treatments of structured probabilistic reasoning in intelligence analysis [151], its application to anomalous aerial observations [152], forensic evidence evaluation [142], and Bayesian network modeling for risk assessment [153].

Case Profile – Toy Example

The composite first draws on accounts during the New Jersey wave.[17] Trained observers reported low-altitude objects moving in coordinated grid patterns over residential areas. The objects were often described to produce "rotor slap," a heavy rhythmic thumping distinct from the high-pitched whir of consumer drones, characteristic of large rotorcraft displacing air with heavy blades. A resident reported one object hovering over a truck at approximately two meters in diameter. The activity repeated on successive evenings, following consistent flight paths. No operator was identified despite investigation by the State Police, FBI, and DHS.

The evidence profile: large-scale aerial objects at low altitude; coordinated grid-pattern flight; acoustic signature consistent with heavy rotorcraft; repeated activity over multiple nights; no identified operator despite federal investigation.

We also include an additional hypothetical observation of rapid, anomalous acceleration of a 'drone' observed near a military base. This was not a something widely reported in the NJ wave itself but is commonly associated with UAP sightings.

[17] Note: While this example is inspired by the NJ Wave, it is meant to be an illustrative toy example and not to draw conclusions about the real NJ-centered events.

Key terms

- **Prior**: what we believe *before* looking at this case's evidence.
- **Relative likelihood**: for one piece of evidence, how well a given hypothesis predicts it, on a simple scale where 1.0 means the evidence tells us nothing about that hypothesis. A value above 1 means the evidence fits that hypothesis; below 1 means it argues against it.
- **Combined weight**: a single running score for each hypothesis, found by multiplying together the relative likelihoods of *all* the evidence.
- **Posterior**: the updated belief *after* the evidence, expressed as a percentage. The posteriors are the numbers a decision-maker actually reads.

Case analysis

We group the observations into a small number of independent evidence items. This grouping matters. Several widely reported facts, that the FAA issued flight restrictions, that nothing was shot down, that the government did not attribute the activity, are not three independent clues; they are three faces of one underlying fact (a cautious, non-attributing official response). Counting them separately would multiply the same signal three times and artificially sharpen the result, so we treat them as one item.

We use three evidence items in total:

- **E1: the civilian observation profile.** What witnesses saw and heard: large objects, low altitude, coordinated grid flight, rotor-slap acoustics, repeated over several nights.
- **E2: the investigation and attribution outcome.** What the official response produced: flight restrictions, no object shot down, and no operator identified despite federal investigation.
- **E3: a single, uncorroborated anomalous-kinematics report** (introduced only in Stage 2): one military sensor logging rapid, propulsion-less acceleration, with no second sensor confirming it.

The numbers below are one analyst's assignment. Different analysts would assign different values, and locating where they differ (a prior? a likelihood?) is exactly what this method is for.

How to read the relative likelihood weights

- ≈ 1.0: evidence is *uninformative* for this hypothesis
- 0.3 – 0.8: mild evidence *against*
- 1.5 – 3: evidence *for*
- ~4: strong evidence *for*

We deliberately cap the weights around 4: no single observation in this toy case is treated as decisive, a constraint whose importance becomes clear in Stage 2. One note on the uniform prior: starting every hypothesis at 20% is a teaching convenience, not a claim of true ignorance. A flat prior treats "unknown phenomenon" (H5) as *a priori* exactly as plausible as "sensor artifact" (H1), which real-world base rates do not support. A genuine assessment would set *context-dependent* priors: the same evidence over an active military base, for instance, would start with far more weight on classified activity (H4).

Stage 1: the reported evidence

We first weigh the two real-world evidence items, the civilian observation profile (E1) and the investigation-and-attribution outcome (E2), to see where the conventional record alone points, before testing what a single anomalous report would do to that picture.

Table 16: Example: Stage 1 – weights and posterior for the civilian observation (E1) and investigation outcome (E2), from a uniform prior.

Hypothesis	E1: civilian observation	E2: investigation outcome	Combined weight (E1 × E2)	Posterior
⊞ H1 Sensor artifact	0.3	1.0	0.30	3%
≈ H2 Natural source	0.3	1.0	0.30	3%
⊠ H3 Human-made (unclassified)	3.0	0.8	2.40	28%
Δ H4 Human-made (classified)	2.5	2.0	5.00	58%
✶ H5 Unknown phenomenon	0.6	1.0	0.60	7%

Following the arithmetic. Take H4: its combined weight is E1 × E2 = 2.5 × 2.0 = **5.00**. Add up all five combined weights, 0.30 + 0.30 + 2.40 + 5.00 + 0.60 = **8.60**, and divide to get each posterior. For H4: 5.00 ÷ 8.60 = 0.58, i.e. **58%**. For H1: 0.30 ÷ 8.60 = 0.035, i.e. about **3%**. *(Percentages are rounded and may not total 100%.)*

Why these weights? The structured, repeating, rotorcraft-like signature is poorly explained by a sensor artifact or a natural source (both well below 1 on E1), and is only mild-evidence *against* an exotic unknown: a genuinely novel phenomenon need not sound like a helicopter. It fits human-made activity well, and the unattributed-despite-investigation outcome (E2) fits classified activity. The result concentrates roughly **86% of the probability on authorized human activity (H3 + H4)**, with the artifact, natural, and unknown hypotheses each small but never driven to zero.

Stage 2: adding one uncorroborated anomalous report

Stage 1's combined weights now become the starting point: carrying a previous result forward as the new prior *is* Bayesian updating. We multiply each by the relative likelihood for the new evidence item E3.

Table 17: Example: Stage 2 – the Stage 1 weights updated by one uncorroborated anomalous report (E3).

Hypothesis	Weight carried from Stage 1	E3: single anomalous sensor observation	New weight	Posterior
⊞ H1 Sensor artifact	0.30	4.0	1.20	12%
≈ H2 Natural source	0.30	0.5	0.15	2%
⊠ H3 Human-made (unclassified)	2.40	0.5	1.20	12%
Δ H4 Human-made (classified)	5.00	1.0	5.00	50%
✶ H5 Unknown phenomenon	0.60	4.0	2.40	24%

Following the arithmetic. Take H5: its new weight is the carried-forward 0.60 × 4.0 = **2.40**. The five new weights total 1.20 + 0.15 + 1.20 + 5.00 + 2.40 = **9.95**, so H5's posterior is 2.40 ÷ 9.95 = **24%**, up from 7%.

The instructive result is what does **not** happen: the unknown hypothesis does not take over. A single sensor reporting impossible kinematics is predicted *equally well* by a sensor artifact (H1) and by a genuine unknown (H5): one instrument alone cannot tell them apart. The distribution becomes **more uncertain, not more exotic**, and classified human technology remains the single leading explanation.

This is the appendix's main lesson, and it echoes the sensor shortcut argument (Figure 5): for the unknown hypothesis (H5) to rise *above* the artifact hypothesis (H1), one needs corroborating evidence that specifically rules the artifact out: independent multi-sensor confirmation. A dramatic single report does not resolve a case toward "unknown"; it widens the range of live possibilities and shows exactly what would narrow them again: independent corroboration from a second sensor.

Appendix I: Historical precedents in anomalous-event communication

The two structural failures, 1) legacy stigma and 2) dismantled protocols, described in the main text are rooted in specific Cold War-era policy decisions. Below we provide additional historical detail.

- **The Robertson Panel and the stigma architecture.** In the summer of 1952, radar-confirmed and visually corroborated objects appeared over Washington, D.C., including over the U.S. Capitol. Widespread press coverage followed, and with it, public concern. In January 1953 the CIA convened a classified scientific review chaired by physicist H. P. Robertson [154]. Its operational recommendation was not investigation but information management: a formal campaign of "debunking" that enlisted media, universities, and scientific institutions to stigmatize the topic and reduce public interest. Officials cited two rationales: preventing public panic and protecting military communication channels from being overwhelmed by civilian reports. An unstated consequence endured far longer than the panic ever could have—a social and professional penalty for reporting anomalous observations that has persisted for seven decades.
- **Project Blue Book and the protocol gap.** From 1952 to 1969, the U.S. Air Force operated Project Blue Book, the only systematic federal program for collecting and analyzing reports of unidentified aerial phenomena. Over seventeen years it compiled more than 12,000 reports. The Condon Report of 1968, a University of Colorado review [155] contracted by the Air Force, concluded that further study was unlikely to produce major scientific advances, and Blue Book was closed in December 1969. Phenomena continued; the program did not. With its closure the government stopped systematically collecting data, dismantled the only inter-agency coordination mechanism for anomalous aerospace events, and left a gap that lasted nearly fifty years. No successor protocol was established until the creation of the All-domain Anomaly Resolution Office (AARO) in 2022.

Appendix J: Observation credibility rating scale for frontline operations

While further analysis into dimensions of credibility could be developed to create a more detailed rating scale for use in scientific investigations [156], we propose two scales of credibility for immediate use in active frontline operations and decision-making [157]. This scale combines several aspects of a detection scenario, including the nature of the detection method (sensor, human observer), their number (single/multiple) or grade (professional/consumer, trained/untrained). A more fine-grained scale specific to human observers is addressed in the next section.

These scales are one input among many and should not gate inclusion. They function as a shared vocabulary and an initial confidence tag for downstream human or AI analysis and are not intended to serve as filters for discarding reports.

Table 18: Credibility rating scale combining multiple aspects of a detection scenario.

Rating	Detection Scenario		
5	Multiple sensors	AND	Multiple human observers
	Example: observation recorded by both radar and FLIR, confirmed from both cockpit and ship bridge		
4	Multiple sensors	AND	Single observer
	Example: cockpit radar and visual observation made by one pilot only		
3	Single sensor	AND/OR	Multiple observers
	Example: radar contact tracked by both cockpit and ATC; or multiple pilots on separate aircraft visually confirm a sighting with no sensor recordings		
2	Single sensor (professional grade)	OR	Single trained observer
	Example: radar contact from ATC only, with no cockpit confirmation or visual sighting		
1	Single sensor (consumer grade)	OR	Single untrained observer
	Example: mobile phone footage captured by one civilian passenger on an aircraft		
0	Error, artefact, hoax		

Human Observer Challenges

Human observers present unique challenges [158] in the context of anomalous incident detection, including:

- Vulnerability to perceptual error, memory distortion, and geometry misjudgment, particularly when they are not trained observers.
- Multiple human observers experiencing different sensory input and processing, resulting in different memories when reporting the same anomalous incident.
- Intentional deception including hoaxes, illusions of the senses, and fabrications.

These challenges may be mitigated by observational training and may be exacerbated by observing conditions particularly for untrained observers. This leads us to the following scale of credibility for human observations to aid the analysis of eyewitness reports.

Table 19: Types of human observers

Rating	Human Observer
5	Military trained observer Example: pilots, radar operators, naval lookouts, air traffic controllers, weapons systems operators
4	Civil aviation trained observer Example: commercial pilots, flight control room personnel
3	Trained non-aviation professional Example: law enforcement, coast guard, meteorologist, air traffic controller acting as visual observer
2	Untrained observer, good conditions Example: general public; daytime, clear skies, unobstructed view
1	Untrained observer, poor conditions Example: general public; night, adverse weather, obstructed or distant view
0	Suspected or confirmed hoaxer Example: known disinformation agent or individual with confirmed history of fabrication

The four types of human observers typically involved in aerial UAP incidents are listed below, in descending order of observational training:

- **Military (rating 5):** witness report by military personnel is often by observers specifically trained to detect and identify classified domestic and foreign military vehicles. However, data accessibility for military witnesses remains restricted due to lack of reporting (stigma or other forms of social pressure) or authorization to speak publicly [159].
- **Civil Aviation (rating 4)**: commercial pilots are trained in air observation including ability to distinguish military, civilian craft and atmospheric phenomena. Pilot eyewitness descriptions include anomaly shape, size, and speed (captured in ATC transcripts). Observations of anomalies in civil aviation have been historically underreported due to stigma and professional consequences to pilots who report anomalous observations [160].

- **Law Enforcement (rating 3)**: state and local law enforcement officers are trained in general visual observation, investigation procedures and reporting, including collection of eye-witness testimony on scene immediately after an incident, collection and analysis of nearby security camera footage, and collection of forensic analysis of physical evidence on scene including biological and material specimens. While they may not be specifically trained for air observation, they may be equipped with relevant methods and tools to reliably capture evidence of anomalous incidents.
- **General Public (rating 1 and 2)**: the general population provides an abundance of visual eyewitness reports. Historically, most of these reports were made to civilian UFO reporting centers such as MUFON, which has a database of 140,000 incidents dating back to 1969. Individual observations of the general public are the most susceptible to the human observer challenges mentioned above, due to the lack of any observational training, including to account for illusory perception due to poor conditions of observation. However, general public eyewitness reports are occasionally high-quality or valuable in any case for aggregate data analysis to derive statistics and trends.

The relevance of human observers should not be underestimated even in contexts concurrently observed by multi-sensor suites. For example, the NASA Artemis II mission, which went around the moon in April 2026, provided unexpected and scientifically valuable eyewitness reports by the crew of micrometeors impact (flashes) on the far side of the moon [161]. This known, natural phenomena, which may be critical for future manned surface mission safety, is hard to image with even the capable camera systems available to the crew. And even when potentially within the capability of the imaging systems, it may be hard to get the timing of the observation right if observing such impact flashes is not the main/only purpose of a mission. The astronauts were also asked to provide information on color hues of the lunar surfaces – subtle variations of color are not easily captured by imaging sensors. Artemis II was a mission equipped with state-of-the-art, calibrated sensors based on the mission profile. Yet, human observers filled the gap of phenomena unobservable or unobserved by even some of the most capable sensors.

References

[1] Federal Bureau of Investigation and U.S. Department of Homeland Security, "Joint DHS/FBI Statement on Reports of Drones in New Jersey," FBI. [Online]. Available: https://www.fbi.gov/news/press-releases/joint-dhs-fbi-statement-on-reports-of-drones-in-new-jersey

[2] J. Harper, "Army seeks more than $400M in fiscal 2025 for systems to counter small drones," *DefenseScoop*, Mar. 11, 2024. [Online]. Available: https://defensescoop.com/2024/03/11/army-counter-drone-systems-funding-fiscal-2025/

[3] Sen. Mike Rounds and Sen. Charles Schumer, *Unidentified Anomalous Phenomena Disclosure Act of 2024*. 2023. doi: 10/text.

[4] Fife Symington, "Symington: I Saw a UFO in the Arizona Sky," *CNN*, Nov. 09, 2007. [Online]. Available: https://www.cnn.com/2007/TECH/science/11/09/simington.ufocommentary/index.html

[5] "Project BLUE BOOK - Unidentified Flying Objects," National Archives. Accessed: Jun. 19, 2026. [Online]. Available: https://www.archives.gov/research/military/air-force/ufos

[6] Dan Farah, *The Age of Disclosure*, (2025). [Online Video]. Available: https://www.theageofdisclosure.com/

[7] W. Westhoven, "They're not our drones, says Picatinny Arsenal. But Morris base confirms sightings," *Daily Record*, Dec. 10, 2024. [Online]. Available: https://www.dailyrecord.com/story/news/2024/12/10/picatinny-arsenal-nj-mystery-drones-not-theirs-sightings/76890630007/

[8] G. Scaduto, "What Really Happened With Last Year's Drone Panic in New Jersey?," *Rolling Stone*, Apr. 04, 2026. [Online]. Available: https://www.rollingstone.com/politics/politics-features/drone-panic-uap-new-jersey-1235531077/

[9] G. Lubold, L. Seligman, and A. Viswanatha, "Mystery Drones Swarmed a U.S. Military Base for 17 Days. The Pentagon Is Stumped," *The Wall Street Journal*, Oct. 12, 2024. [Online]. Available: https://www.wsj.com/politics/national-security/military-base-drones-mystery-1722d4a8

[10] B. Stewart, "ANALYSIS | Mysterious Drones Keep Buzzing Key Sites in Europe. So What's the Defence Strategy?," *CBC News*, Nov. 11, 2025. [Online]. Available: https://www.cbc.ca/news/world/drones-belgium-europe-russia-9.6973910

[11] Air Force Global Strike Command, "FACT CHECK: Barksdale Drone Incursion." [Online]. Available: https://www.afgsc.af.mil/News/Article-Display/Article/4448052/fact-check-barksdale-drone-incursion/

[12] J. Margolin and Aaron Katersky, "'Multiple Waves' of Unauthorized Drones Recently Spotted Over Strategic US Air Force Base," *ABC News*, Mar. 20, 2026. [Online]. Available: https://abcnews.com/International/multiple-waves-unauthorized-drones-spotted-strategic-us-air/story?id=131245527

[13] J. Malaska, "Phantom Swarm, Part 1: The Official Story," John Malaska. Accessed: Jun. 21, 2026. [Online]. Available: https://jmalaska.substack.com/p/phantom-swarm-part-1-the-official

[14] J. Miller, *TELL: a weak-signal detection pipeline for ambiguous information environments*. (Jun. 13, 2026). Zenodo. doi: 10.5281/ZENODO.20681167.

[15] "Congressman Van Drew Warns of National Security Threat from Drones, Calls for Them to Be Shot Down," U.S. Congressman Jefferson Van Drew. Accessed: Jun. 23, 2026. [Online]. Available: https://vandrew.house.gov/news/documentsingle.aspx?DocumentID=1788

[16] Ian W. Evett, "Interpretation: A Personal Odyssey," in *The Use of Statistics in Forensic Science*, C.G.G. Aitken and David A. Stoney, Eds., Chichester: Ellis Horwood, 1991, pp. 9–22.

[17] R. M. Medina, S. C. Brewer, and S. M. Kirkpatrick, "An Environmental Analysis of Public UAP Sightings and Sky View Potential," *Sci. Rep.*, vol. 13, Dec. 2023, doi: 10.1038/s41598-023-49527-x.

[18] U.S. Army Small Business Innovation Research (SBIR) Program, "Miniaturization of Hyperspectral Sensors for UAS Applications," U.S. Army SBIR. [Online]. Available: https://armysbir.army.mil/topics/miniaturization-hyperspectral-sensors-uas-applications/

[19] TEKEVER, "TEKEVER and Arkeus Integrate Warden Hyperspectral Sensor to Enhance Long-Range Detection and Mission Effectiveness," *UAS Magazine*, Nov. 12, 2025. [Online]. Available: https://uasmagazine.com/articles/tekever-and-arkeus-integrate-warden-hyperspectral-sensor-to-enhance-long-range-detection-and-mission-effectiveness

[20] L. Dominé *et al.*, "Commissioning an All-Sky Infrared Camera Array for Detection of Airborne Objects," *Sensors*, vol. 25, no. 3, 2025, doi: 10.3390/s25030783.

[21] M. Schneider, L. Halekotte, T. Comes, D. Lichte, and F. Fiedrich, "Emergency Response Inference Mapping (ERIMap): A Bayesian Network-Based Method for Dynamic Observation Processing in Spatially Distributed Emergencies," *Reliab. Eng. Syst. Saf.*, vol. 255, 2025, doi: 10.1016/j.ress.2024.110640.

[22] John M. Aronis, Ye Ye, Jessi Espino, Harry Hochheiser, Marian G. Michaels, and Gregory F. Cooper, "A Bayesian System to Detect and Track Outbreaks of Influenza-Like Illnesses Including Novel Diseases: Algorithm Development and Validation," *JMIR Public Health Surveill.*, vol. 10, 2024, doi: 10.2196/57349.

[23] Naveed Ejaz and Salimur Choudhury, "A Comprehensive Survey of the Machine Learning Pipeline for Wildfire Risk Prediction and Assessment," *Ecol. Inform.*, vol. 90, 2025, doi: 10.1016/j.ecoinf.2025.103325.

[24] Andrea Pinto, Luis-Carlos Herrera, Yezid Donoso, and Jairo A. Gutierrez, "Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure," *Sensors*, vol. 23, no. 5, 2023, doi: 10.3390/s23052415.

[25] Xiaoming Liu, Jun Liu, Yu Zhao, Tao Ding, Xinglei Liu, and Jiacheng Liu, "A Bayesian Deep Learning-Based Probabilistic Risk Assessment and Early-Warning Model for Power Systems Considering Meteorological Conditions," *IEEE Trans. Ind. Inform.*, vol. 20, no. 2, pp. 1516–1527, 2024, doi: 10.1109/TII.2023.3278873.

[26] Mengjun Meng, Qiuyun Lin, and Yingming Wang, "The Risk Assessment of Manufacturing Supply Chains Based on Bayesian Networks with Uncertainty of Demand," *J. Intell. Fuzzy Syst.*, vol. 42, no. 6, pp. 5753–5771, 2022, doi: 10.3233/JIFS-212207.

[27] Thomas S. Ferguson, "A Bayesian Analysis of Some Nonparametric Problems," *Ann. Stat.*, vol. 1, no. 2, pp. 209–230, Mar. 1973, doi: 10.1214/aos/1176342360.

[28] Yee Whye Teh, Michael I. Jordan, Matthew J. Beal, and David M. Blei, "Hierarchical Dirichlet Processes," *J. Am. Stat. Assoc.*, vol. 101, no. 476, pp. 1566–1581, 2006, doi: 10.1198/016214506000000302.

[29] Forcys, "Sentinel IDS - Intruder Detection Sonar," Forcys. [Online]. Available: https://www.forcys.com/instruments/sentinel-ids/

[30] Teledyne Marine, "2D Forward Looking Sonar Systems," Teledyne Marine. [Online]. Available: https://www.teledynemarine.com/products/product-line/sonar/forward-looking-imaging-sonars

[31] Robin Radar, "Protecting Oil Rigs from Drones with Counter-UAS Radar," Robin Radar. [Online]. Available: https://www.robinradar.com/blog/protecting-oil-rigs-from-drones-with-counter-uas-radar

[32] HENSOLDT, "Security Surveillance Radars," HENSOLDT. [Online]. Available: https://www.hensoldt.net/domains/land/istar/security-surveillance-radars

[33] Swiss BirdRadar, "Radar System BirdScan MV1," Swiss BirdRadar. [Online]. Available: https://swissbirdradar.com/systems/radar-birdscan-mv1/

[34] IdentiFlight, "IdentiFlight - Bird Detection System," IdentiFlight. [Online]. Available: https://www.identiflight.com/

[35] DeTect, Inc., "Wind Energy Bird Radar + Real-time Platform," DeTect, Inc. [Online]. Available: https://detect-inc.com/wind-energy-bird-bat-radars/

[36] Flowco, "Aerial Methane Leak Detection," Flowco. [Online]. Available: https://www.flowcoinc.com/products-services/methane-leak-detection/aerial

[37] A. Fascista, "Toward Integrated Large-Scale Environmental Monitoring Using WSN/UAV/Crowdsensing: A Review of Applications, Signal Processing, and Future Perspectives," *Sensors*, vol. 22, no. 5, 2022, doi: 10.3390/s22051824.

[38] D. B. Olawade, O. Z. Wada, A. O. Ige, B. I. Egbewole, A. Olojo, and B. I. Oladapo, "Artificial Intelligence in Environmental Monitoring: Advancements, Challenges, and Future Directions," *Hyg. Environ. Health Adv.*, vol. 12, Dec. 2024, doi: 10.1016/j.heha.2024.100114.

[39] United States Space Force, "Commercial Space Strategy," United States Space Force, Apr. 2024. Accessed: Jun. 21, 2026. [Online]. Available: https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf

[40] NOAA Office of Space Commerce, "Traffic Coordination System for Space (TraCSS)." Accessed: Jun. 21, 2026. [Online]. Available: https://space.commerce.gov/traffic-coordination-system-for-space-tracss/

[41] NASA Orbital Debris Program Office, "Debris Measurements." Accessed: Jun. 21, 2026. [Online]. Available: https://orbitaldebris.jsc.nasa.gov/measurements/

[42] L. Zhou, "What's up with all these drone sightings?," *Vox*, Dec. 17, 2024. [Online]. Available: https://www.vox.com/politics/391335/391335

[43] John Joseph Tedesco and Gerald Thomas Tedesco, "Eye on the Sky: A UAP Research and Field Study off New York's Long Island Coast," *Open J. Appl. Sci.*, vol. 14, no. 8, pp. 2267–2295, Aug. 2024, doi: 10.4236/ojapps.2024.148152.

[44] M. Phelan, "How These Two Brothers Became Go-to Experts on America's 'Mystery Drone' Invasion," *MIT Technology Review*, Aug. 26, 2025. [Online]. Available: https://www.technologyreview.com/2025/08/26/1121458/ufo-hunters-mystery-drone-invasion/

[45] R. Olch, "What Is the UFO Data Acquisition Project?," presented at the SCU Anomalous Aerospace Phenomena Conference, Jun. 2021. Accessed: Jun. 14, 2026. [Online]. Available: https://ufodap.com/

[46] "Congressman Van Drew Addresses Ongoing Drone Incursions," U.S. Congressman Jefferson Van Drew. Accessed: Jun. 23, 2026. [Online]. Available: https://vandrew.house.gov/news/documentsingle.aspx?DocumentID=1792

[47] R. L. Weaver and J. McAndrew, "The Roswell Report: Fact versus Fiction in the New Mexico Desert,:," Defense Technical Information Center, Fort Belvoir, VA, Jan. 1995. doi: 10.21236/ADA326148.

[48] J. A. Hynek, *The UFO Experience: A Scientific Inquiry*.

[49] Helene Cooper, Ralph Blumenthal, and Leslie Kean, "Glowing Auras and 'Black Money': The Pentagon's Mysterious U.F.O. Program," *New York Times*, Dec. 16, 2017. [Online]. Available: https://www.nytimes.com/2017/12/16/us/politics/pentagon-program-ufo-harry-reid.html

[50] M. Hanks, "AARO's Historical Report: A Tale of Factual Errors and Old Mistakes Repeated," *The Debrief*, Mar. 14, 2024. [Online]. Available: https://thedebrief.org/aaros-historical-report-a-tale-of-factual-errors-and-old-mistakes-repeated/

[51] M. E. Yingling and C. W. Yingling, "Academic Freedom and the Unknown: Credibility, Criticism, and Inquiry among the Professoriate," *Humanit. Soc. Sci. Commun.*, vol. 11, 2024, doi: 10.1057/s41599-024-03351-4.

[52] A. Wu, "Focused Research Organizations: A New Model for Scientific Research," Federation of American Scientists. [Online]. Available: https://fas.org/publication/focused-research-organizations-a-new-model-for-scientific-research/

[53] Wesley Andrés Watters *et al.*, "The Scientific Investigation of Unidentified Aerial Phenomena (UAP) Using Multimodal Ground-Based Observatories," *J. Astron. Instrum.*, vol. 12, no. 1, 2023, doi: 10.1142/S2251171723400068.

[54] AARO, "2025 UAP Workshop: Narrative Data, Infrastructures, and Analysis," All-domain Anomaly Resolution Office, 2025. [Online]. Available: https://www.aaro.mil/Portals/136/PDFs/Information%20Papers/2025_UAP_Workshop_Paper.pdf

[55] NASA Unidentified Anomalous Phenomena Independent Study Team, "UAP Independent Study Team Final Report," science.nasa.gov, Sep. 2023. [Online]. Available: https://science.nasa.gov/wp-content/uploads/2023/09/uap-independent-study-team-final-report.pdf

[56] International Science Reserve, "What We Do," International Science Reserve. [Online]. Available: https://isr.nyas.org/what-we-do/

[57] ProPublica, "Rx Inspector," ProPublica. [Online]. Available: https://projects.propublica.org/rx-inspector/

[58] Cochrane, "Plain Language Summaries," Cochrane Evidence. [Online]. Available: https://www.cochrane.org/evidence

[59] Foteini Vervelidou *et al.*, "The Deployment of a Geomagnetic Variometer Station as Auxiliary Instrumentation for the Study of Unidentified Aerial Phenomena," *Geosci. Instrum. Methods Data Syst.*, vol. 14, pp. 335–351, 2025, doi: 10.5194/gi-14-335-2025.

[60] M. West, "'Green Pyramid' UFOs in Night Vision Footage Are Bokeh," Metabunk. [Online]. Available: https://www.metabunk.org/threads/green-pyramid-ufos-in-night-vision-footage-are-bokeh.11695/

[61] Stephen Bruehl and Beatriz Villarroel, "Transients in the Palomar Observatory Sky Survey (POSS-I) May Be Associated with Nuclear Testing and Reports of Unidentified Anomalous Phenomena," *Sci. Rep.*, vol. 15, Oct. 2025, doi: 10.1038/s41598-025-21620-3.

[62] Beatriz Villarroel, Iñigo Imaz, and Josefine Bergstedt, "Our Sky Now and Then: Searches for Lost Stars and Impossible Effects as Probes of Advanced Extraterrestrial Civilizations," *Astron. J.*, vol. 152, no. 3, 2016, doi: 10.3847/0004-6256/152/3/76.

[63] B. Vincent, "DOD developing 'Gremlin' capability to help personnel collect real-time UAP data," *DefenseScoop*, Mar. 08, 2024. Accessed: Jun. 21, 2026. [Online]. Available: https://defensescoop.com/2024/03/08/embargo-10a-friday-dod-developing-gremlin-capability-to-help-personnel-collect-real-time-uap-data/

[64] M. Szydagis, K. H. Knuth, B. W. Kugielsky, and C. Levy, "Initial Results from the First Field Expedition of UAPx to Study Unidentified Anomalous Phenomena," *Prog. Aerosp. Sci.*, vol. 156, 2025, doi: 10.1016/j.paerosci.2025.101099.

[65] Skywatcher, "Skywatcher: Defining The Future of Aerial Intelligence," Skywatcher. Accessed: Jun. 21, 2026. [Online]. Available: https://skywatcher.ai/

[66] Tyler Rogoway and Joseph Trevithick, "The Night a Mysterious Drone Swarm Descended on Palo Verde Nuclear Power Plant," *The War Zone*, Jul. 30, 2020. [Online]. Available: https://www.twz.com/34800/the-night-a-drone-swarm-descended-on-palo-verde-nuclear-power-plant

[67] J. Williams, "Nebraska Congressman Weighs-In on Mysterious Drone Sightings," *Nebraska Public Media News*, Jan. 07, 2020. [Online]. Available: https://nebraskapublicmedia.org/en/news/news-articles/nebraska-congressman-weighs-in-on-mysterious-drone-sightings/

[68] B. Tingley, "Newly Released FAA Documents Give Unprecedented Look into Colorado Drone Swarm Mystery," *The War Zone*, Jul. 16, 2020. [Online]. Available: https://www.twz.com/34662/faa-documents-offer-unprecedented-look-into-colorado-drone-mystery

[69] PBS NewsHour, "U.S. Reveals New Details About Flying Objects and Decision to Shoot Them Down," *PBS NewsHour*, Feb. 13, 2023. [Online]. Available: https://www.pbs.org/newshour/show/u-s-reveals-new-details-about-flying-objects-and-decision-to-shoot-them-down

[70] B. Whitaker, "How the U.S. Is Confronting the Threat Posed by Drones Swarming Sensitive National Security Sites," *60 Minutes, CBS News*, Jun. 29, 2025. [Online]. Available: https://www.cbsnews.com/news/drone-swarms-national-security-60-minutes-transcript-2025-06-29/

[71] Joseph Trevithick and Howard Altman, "Palmdale UFO Scare Leads to Revelations About Mystery Drone Incursions Over Secretive Plant 42," *The War Zone*, Aug. 19, 2024. [Online]. Available: https://www.twz.com/air/palmdale-ufo-scare-leads-to-revelations-about-mystery-drone-incursions-over-secretive-plant-42

[72] Kyle Warfel and Christopher Sharp, "Newly Obtained USAF Reports Expose Drone Breaches at Plant 42, Home to B-21 Raider and Other Top Secret Programs, Sparking Espionage Concerns," *Liberation Times*, Feb. 12, 2025. [Online]. Available: https://www.liberationtimes.com/home/newly-obtained-usaf-reports-expose-drone-breaches-at-plant-42-home-to-b-21-raider-and-other-top-secret-programs-sparking-espionage-concerns

[73] M. de la Baume, "Unidentified Drones Are Seen Above French Nuclear Plants," *The New York Times*, Nov. 04, 2014. [Online]. Available: https://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html

[74] S. Shackle, "The Mystery of the Gatwick Drone," *The Guardian*, Dec. 01, 2020. [Online]. Available: https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone

[75] Reuters, "Swedish Security Service Investigates Drones at Three Nuclear Plants," *Reuters*, Jan. 17, 2022. [Online]. Available: https://www.reuters.com/world/europe/swedish-security-service-investigates-drones-three-nuclear-plants-2022-01-17/

[76] BBC News, "Sweden Drones: Sightings Reported over Nuclear Plants and Palace," *BBC*, Jan. 18, 2022. [Online]. Available: https://www.bbc.com/news/world-europe-60035446

[77] Associated Press, "Gatwick airport shuts runway after reports of nearby drone activity," *AP News*, May 14, 2023. [Online]. Available: https://apnews.com/article/gatwick-airport-london-closed-drone-0ba52e1a78607b6a7efa48c69b6c7dcc

[78] Reuters, "No Evidence New Jersey Drone Sightings Pose Security Threat, White House Says," *Reuters*, Dec. 12, 2024. [Online]. Available: https://www.reuters.com/world/us/no-evidence-new-jersey-drone-sightings-pose-security-threat-white-house-says-2024-12-12/

[79] Tina Kelley, "After Nighttime Flights, FAA Bans Drones over Trump's NJ Golf Course," *NJ.com*, Dec. 03, 2024. [Online]. Available: https://www.nj.com/morris/2024/12/after-nighttime-flights-faa-bans-drones-over-trumps-nj-golf-course.html

[80] M. Petti, "Newly Released Documents Show What the Feds Knew About the New Jersey Drone Scare," *Reason*, May 09, 2025. [Online]. Available: https://reason.com/2025/05/09/what-the-feds-knew-about-the-new-jersey-drone-scare/

[81] Federal Bureau of Investigation, Newark Field Office, "FBI Newark Seeks Information on Drone Sightings," FBI. [Online]. Available: https://www.fbi.gov/contact-us/field-offices/newark/news/fbi-newark-seeks-information-on-drone-sightings

[82] R. Herd and Morris County Mayors, "Letter to Governor Phil Murphy regarding unidentified drone sightings over Morris County," Dec. 08, 2024. [Online]. Available: https://www.riverdalenj.gov/_Content/pdf/Morris-County-Mayors-Letter-to-Governor-Dec2024.pdf

[83] "Mayors Left Frustrated Following Meeting Regarding New Jersey Drone Sightings," News 12 Long Island, Dec. 11, 2024. [Online]. Available: https://longisland.news12.com/2024/12/11/mayors-left-frustrated-following-meeting-regarding-new-jersey-drone-sightings/5XfnbglId2jItazdVaQ6Nh

[84] Bruce Shipkowski, "Homeland Security shares new details of mysterious drone flights over New Jersey," *AP News*, Dec. 12, 2024. [Online]. Available: https://apnews.com/article/fbi-drones-new-jersey-a978470fa3bb07ed3e98c5b7c18f0abb

[85] I. Ali and P. Stewart, "No Iranian Drone 'Mothership' off the United States Launching Drones, Pentagon Says," *Reuters*, Dec. 11, 2024. [Online]. Available: https://www.reuters.com/world/us/no-iranian-drone-mothership-off-united-states-launching-drones-pentagon-says-2024-12-11/

[86] Chris Harris, "NJ's Largest Utility Firm Begs Feds to Shut Down Airspace over Nuclear Plant as Mystery Drones Spotted," *New York Post*, Dec. 14, 2024. [Online]. Available: https://nypost.com/2024/12/14/us-news/njs-largest-utility-firm-begs-feds-to-shut-down-airspace-over-nuclear-plant-as-mystery-drones-spotted/

[87] P. Reilly, "NJ Navy Base Confirms Multiple Drones Entered Its Airspace," *New York Post*, Dec. 13, 2024. [Online]. Available: https://nypost.com/2024/12/13/us-news/nj-navy-base-confirms-multiple-drones-entered-its-airspace/

[88] Office of the Governor of New York, "Statement from Governor Kathy Hochul on Additional Drone Activity," Governor Kathy Hochul. [Online]. Available: https://www.governor.ny.gov/news/statement-governor-kathy-hochul-additional-drone-activity

[89] Office of Representative Pat Ryan, "Following Shutdown of Stewart Airport, Congressman Pat Ryan Slams Lack of Urgency and Transparency on Drone Sightings, Calls for Additional Public Disclosure, Overhaul of Counter-UAS Protocol," Congressman Pat Ryan. [Online]. Available: https://patryan.house.gov/media/press-releases/following-shutdown-stewart-airport-congressman-pat-ryan-slams-lack-urgency-and

[90] Admin, "Two Suspects Arrested Following Hazardous Drone Operation on Long Island," Boston Police Department. [Online]. Available: https://police.boston.gov/2024/12/15/two-suspects-arrested-following-hazardous-drone-operation-on-long-island/

[91] Dave Collins and Mike Catalini, "Drone Detectors in N.J. Find 'Little or No Evidence' of Wrongdoing, Governor Says," *AP News*, Dec. 2024. [Online]. Available: https://apnews.com/article/drones-mystery-new-jersey-york-b37fda04755803392178b1f39b76ccd8

[92] D. Shepardson, "FAA Banning Drone Flights over Critical Infrastructure Locations in New Jersey," *Reuters*, Dec. 19, 2024. [Online]. Available: https://www.reuters.com/world/us/faa-banning-drone-flights-over-critical-infrastructure-locations-new-jersey-2024-12-19/

[93] Office of Sen. Chuck Schumer, "Leader Schumer Demands Answers on Mystery Drones Across New York, New Jersey and the Northeast; Urges Immediate Deployment of State-of-the-Art Drone Technology to Get to the Bottom of Mystery; Will Call for Passage of Legislation That Gives Local Leaders More Tools ASAP," Senate Democrats. [Online]. Available: https://www.democrats.senate.gov/newsroom/press-releases/leader-schumer-demands-answers-on-mystery-drones-across-new-york-new-jersey-and-the-north-east-urges-immediate-deployment-of-state-of-the-art-drone-technology-to-get-to-the-bottom-of-mystery-will-call-for-passage-of-legislation-that-gives-local-leaders-more-tools-asap

[94] Department of Homeland Security, Federal Bureau of Investigation, Federal Aviation Administration, and Department of Defense, "DHS, FBI, FAA & DoD Joint Statement on Ongoing Response to Reported Drone Sightings," FAA Newsroom. [Online]. Available: https://www.faa.gov/newsroom/dhs-fbi-faa-dod-joint-statement-ongoing-response-reported-drone-sightings

[95] Edward Helmore, "Mayorkas Says No Known Foreign Involvement in North-East Drone Sightings," *The Guardian*, Dec. 15, 2024. [Online]. Available: https://www.theguardian.com/us-news/2024/dec/15/mayorkas-north-east-drone-sightings

[96] Flynn Nicholls, "Joe Biden Breaks Silence on Mystery Drones," *Newsweek*, Dec. 18, 2024. [Online]. Available: https://www.newsweek.com/joe-biden-breaks-silence-mystery-drones-2002573

[97] U.S. Nuclear Regulatory Commission, "Event Notification Report for December 2, 2024," Nuclear Regulatory Commission, Dec. 2024. [Online]. Available: https://www.nrc.gov/reading-rm/doc-collections/event-status/event/2024/20241202en.html

[98] M. Glasser and Leah Sarnoff, "Drones Were Not Tracking Missing Radioactive Material in New Jersey, DEP Says," *6abc Philadelphia*, Dec. 18, 2024. [Online]. Available: https://6abc.com/post/fact-check-drones-were-not-tracking-missing-radioactive-material-new-jersey-department-energy-related-officials-say/15670972/

[99] Associated Press, "Federal officials' authority to track and disable drones set to expire," *AP News*, Dec. 19, 2024. [Online]. Available: https://apnews.com/article/drones-mystery-new-jersey-york-congress-54c73bba3352c05d9191cf84b3acb2a4

[100] Anna Betts, "White House Says New Jersey Drones 'Authorized to Be Flown by FAA,'" *The Guardian*, Jan. 28, 2025. [Online]. Available: https://www.theguardian.com/us-news/2025/jan/28/karoline-leavitt-new-jersey-drones

[101] U.S. Air Forces in Europe – Air Forces Africa Public Affairs, "U.S. Air Forces in Europe - Air Forces Africa Statement on Installation Security in the UK (Update 1)," U.S. Air Forces in Europe - Air Forces Africa. [Online]. Available: https://www.usafe.af.mil/News/Press-Releases/Display/Article/3976904/us-air-forces-in-europe-air-forces-africa-statement-on-installation-security-in

[102] Sarah Young, Catarina Demony, Idrees Ali, and Phil Stewart, "US Air Force Says Drones Spotted over Its Military Bases in England," *Reuters*, Nov. 26, 2024. [Online]. Available: https://www.reuters.com/world/us-air-force-says-drones-spotted-over-its-military-bases-england-2024-11-26/

[103] "UK Air and Missile Defences." Hansard, House of Commons Debates, Nov. 27, 2024. [Online]. Available: https://hansard.parliament.uk/commons/2024-11-27/debates/3D4A0ABD-99E8-4955-A7A9-50E4D25C281F/UKAirAndMissileDefences

[104] "Daily Report: Thursday, 12 June 2025." Jun. 12, 2025. [Online]. Available: https://qna.files.parliament.uk/qnadailyreports/Written-Questions-Answers-Statements-Daily-Report-Commons-2025-06-12.pdf

[105] U.S. Attorney's Office, Central District of California, "Northern California Man Arrested for Allegedly Flying Drone over and Photographing Vandenberg Space Force Base," United States Department of Justice. [Online]. Available: https://www.justice.gov/usao-cdca/pr/brentwood-man-arrested-allegedly-flying-drone-over-and-photographing-vandenberg-space

[106] Andreas Rinke and Rachel More, "Unidentified Drones Sighted over US Air Base in Germany, Spiegel Reports," *Reuters*, Dec. 13, 2024. [Online]. Available: https://www.reuters.com/world/europe/unidentified-drones-sighted-over-us-air-base-germany-spiegel-reports-2024-12-13/

[107] Howard Altman, "Multiple Drone Incursions Confirmed Over Marine Corps Base Camp Pendleton (Updated)," *The War Zone*, Dec. 17, 2024. [Online]. Available: https://www.twz.com/news-features/multiple-drone-incursions-reported-over-marine-corps-base-camp-pendleton

[108] T. Weingartner, "Wright-Patt's Airspace Briefly Shut Down Because of Drone Activity," *WYSO*, Dec. 15, 2024. [Online]. Available: https://www.wyso.org/2024-12-15/wright-patterson-air-force-base-drones

[109] 88th Air Base Wing Public Affairs, "Wright-Patt Airspace Experiences Additional Drone Incursions," Wright-Patterson Air Force Base. [Online]. Available: https://www.wpafb.af.mil/News/Article-Display/Article/4015684/wright-patt-airspace-experiences-additional-drone-incursions/

[110] C. Ballard, "Utah's Hill Air Force Base Confirms Drone Sightings," *KUER*, Dec. 16, 2024. [Online]. Available: https://www.kuer.org/politics-government/2024-12-16/utahs-hill-air-force-base-confirms-drone-sightings

[111] "Suspicious Drone Activity Reported in North Texas near Military Sites, Authorities Say," CBS News Texas, Dec. 19, 2024. [Online]. Available: https://www.cbsnews.com/texas/news/white-settlement-federal-officials-address-suspicious-drone-activity-near-military-sites/

[112] S. Siebold, "German Police Investigate Suspected Russian Espionage at Military Bases," *Reuters*, Jan. 13, 2025. [Online]. Available: https://www.reuters.com/world/europe/german-police-investigate-suspected-russian-espionage-military-bases-2025-01-13/

[113] "To Receive Testimony on the Posture of United States Northern Command and United States Southern Command in Review of the Defense Authorization Request for Fiscal Year 2026 and the Future Years Defense Program." Feb. 13, 2025. [Online]. Available: https://www.armed-services.senate.gov/imo/media/doc/02-13-2025-full-transcript.pdf

[114] Louise Rasmussen, "Norway Police End Oslo Airport Drone Probe, Citing Lack of Evidence," *Reuters*, Nov. 06, 2025. [Online]. Available: https://www.reuters.com/world/norway-police-end-oslo-airport-drone-probe-citing-lack-evidence-2025-11-06/

[115] Livia Albeck-Ripka, Francesca Regalado, Maya Tekeli, and Lynsey Chutel, "Copenhagen and Oslo Airports Closed by Drone Sightings," *The New York Times*, Sep. 22, 2025. [Online]. Available: https://www.nytimes.com/2025/09/22/world/europe/copenhagen-oslo-airport-closed-drone.html

[116] Reuters, "Denmark Links Drone Sorties to State Actor, Latvia Says; Russia Denies Involvement," *Reuters*, Sep. 25, 2025. [Online]. Available: https://www.reuters.com/world/europe/denmark-reopens-airports-after-drone-disruption-2025-09-25/

[117] Defence Command Denmark, "Regarding Drones over Denmark," Danish Armed Forces. [Online]. Available: https://www.forsvaret.dk/en/news/2025/dronesoverdenmark/

[118] Rigspolitiet, "Mere End 500 Droneanmeldelser på Nationalt Plan i Det Seneste Døgn," *Politi*, Sep. 26, 2025. [Online]. Available: https://politi.dk/rigspolitiet/nyhedsliste/mere-end-500-droneanmeldelser-paa-nationalt-plan-i-det-seneste-doegn/2025/09/26

[119] Associated Press, "Mystery Drone Sightings Reported over Critical Infrastructure in Northern Germany," *AP News*, Oct. 01, 2025. [Online]. Available: https://apnews.com/article/germany-drone-critical-infrastructure-russia-nato-investigation-a9670df4bfe877b54094b7894aa125a5

[120] Associated Press, "A drone flyover above Copenhagen Airport prompts concerns that Russia was behind it," *AP News*, Sep. 23, 2025. [Online]. Available: https://apnews.com/article/drone-denmark-police-security-8e8119cfbc0e276cee1f37ff5ead11d8

[121] Reuters, "Denmark Bans Drone Flights after Fresh Drone Sightings at Military Bases," *Reuters*, Sep. 28, 2025. [Online]. Available: https://www.reuters.com/world/denmark-bans-drone-flights-after-fresh-drone-sightings-military-bases-2025-09-28

[122] Reuters, "Denmark Says New Drone Sightings Overnight at Military Installations," *Reuters*, Sep. 27, 2025. [Online]. Available: https://www.reuters.com/world/denmark-says-new-drone-sightings-overnight-military-installations-2025-09-27/

[123] Y. Porokhnia, "In Norway, a Passenger Plane Was Turned around Because of an Unknown Drone over the Airport," *LIGA.net*, Sep. 29, 2025. [Online]. Available: https://news.liga.net/en/politics/news/in-norway-a-passenger-plane-was-turned-around-because-of-an-unknown-drone-over-the-airport

[124] Stella Bugge, Elise Kvien, and Hege Varsi, "Norwegian-Fly til Bardufoss Snudde Etter Droneobservasjoner," *VG*, Sep. 28, 2025. [Online]. Available: https://www.vg.no/nyheter/i/4Byga9/avinor-observasjon-av-drone-innen-forbudssonen-til-broennoeysund-lufthavn

[125] T. Lanchukovska, "An Unknown Drone Was Spotted over a Hydroelectric Power Plant in Finland," *LIGA.net*, Sep. 27, 2025. [Online]. Available: https://news.liga.net/en/world/news/an-unknown-drone-was-spotted-over-a-hydroelectric-power-plant-in-finland

[126] K. Strohecker and J. Poltz, "Multiple Drone Sightings Reported in Germany in Past Three Days, Bild Says," *Reuters*, Oct. 04, 2025. [Online]. Available: https://www.reuters.com/business/aerospace-defense/munich-runways-closed-again-pilot-blames-drone-sightings-2025-10-03/

[127] Sarah Marsh and Andreas Rinke, "Germany to Allow Police to Shoot Down Drones," *Reuters*, Oct. 08, 2025. [Online]. Available: https://www.reuters.com/business/aerospace-defense/germany-allow-police-shoot-down-drones-2025-10-08/

[128] Alessandro Parodi, "Belgium Investigates New Drone Sightings over Military Base," *Reuters*, Oct. 29, 2025. [Online]. Available: https://www.reuters.com/world/belgium-investigates-new-drone-sightings-over-military-base-2025-10-29/

[129] Associated Press, "A Drone Sighting Temporarily Suspends Air Travel at the Berlin Airport," *AP News*, Nov. 01, 2025. [Online]. Available: https://apnews.com/article/berlin-airport-drone-germany-233028211d399bbbbbca72a08a767ef3

[130] Agence France-Presse, "Flights Resume at Berlin Airport After Suspension over Drone Scare," *France 24*, Nov. 01, 2025. [Online]. Available: https://www.france24.com/en/europe/20251101-flights-resume-at-berlin-airport-after-suspension-over-drone-scare

[131] Siddharth Philip and Benedikt Kammel, "Berlin Airport Briefly Closed in Latest Drone Disruption," *Bloomberg*, Oct. 31, 2025. [Online]. Available: https://www.bloomberg.com/news/articles/2025-10-31/berlin-airport-briefly-closed-in-latest-drone-disruption

[132] CNN, "Drones Spotted over Belgian Airbase Spark Espionage Concerns," *CNN*, Nov. 02, 2025. [Online]. Available: https://www.cnn.com/2025/11/02/europe/drones-spotted-belgian-airbase-spying

[133] Charlotte Van Campenhout, "Brussels Airport Temporarily Halted Operations Due to Drone Sighting," *Reuters*, Nov. 06, 2025. [Online]. Available: https://www.reuters.com/business/aerospace-defense/brussels-airport-temporarily-halted-operations-due-drone-sighting-2025-11-06/

[134] Politico Europe, "Belgium Flounders as 5 Drones Buzz Nuclear Power Plant," *Politico Europe*, Nov. 10, 2025. [Online]. Available: https://www.politico.eu/article/drones-spotted-belgium-nuclear-plant-doel-airspace-incursions/

[135] L. Bayer and P. Blenkinsop, "Belgium Enlists Foreign Forces to Combat Drone Incursions," *Reuters*, Nov. 10, 2025. [Online]. Available: https://www.reuters.com/world/belgium-enlists-foreign-forces-combat-drone-incursions-2025-11-10/

[136] Charlotte Van Campenhout, "Belgium to Deploy Air-Defence System in Antwerp Port to Counter Drone Threats," *Reuters*, Feb. 26, 2026. [Online]. Available: https://www.reuters.com/business/aerospace-defense/belgium-install-airdefence-system-port-antwerp-2027-newspaper-says-2026-02-26/

[137] Johan Ahlander, "Traffic Halted at Swedish City Gothenburg's Airport after Drone Sighting," *Reuters*, Nov. 06, 2025. [Online]. Available: https://www.reuters.com/world/traffic-halted-swedish-city-gothenburgs-airport-after-drone-sighting-daily-2025-11-06/

[138] Reuters, "Dutch Military Uses Weapons against Drones over Air Force Base," *Reuters*, Nov. 22, 2025. [Online]. Available: https://www.reuters.com/world/dutch-military-uses-weapons-against-drones-over-air-force-base-2025-11-22/

[139] Reuters, "Drone Sightings Disrupt Traffic at Eindhoven Airport," *Reuters*, Nov. 22, 2025. [Online]. Available: https://www.reuters.com/business/aerospace-defense/eindhoven-airport-closed-after-drone-sightings-defence-minister-says-2025-11-22/

[140] Reuters, "Netherlands Buys Drone Detection Radars after Recent Sightings," *Reuters*, Nov. 27, 2025. [Online]. Available: https://www.reuters.com/business/aerospace-defense/netherlands-buys-drone-detection-radars-after-recent-sightings-2025-11-27/

[141] Le Parisien and Agence France-Presse, "Dordogne: Nouveau Survol d'une Usine d'Armement par un Drone," *Le Parisien*, Nov. 13, 2025. [Online]. Available: https://www.leparisien.fr/faits-divers/dordogne-nouveau-survol-dune-usine-darmement-par-un-drone-13-11-2025-QPAZA2QPXFEI5IOM-WSTLE6PO2A.php

[142] Le Monde and Agence France-Presse, "French Police Investigate after Drone Flies over Tank Convoy," *Le Monde*, Nov. 12, 2025. [Online]. Available: https://www.lemonde.fr/en/international/article/2025/11/12/french-police-investigate-after-drone-flies-over-tank-convoy_6747392_4.html

[143] Louise Rasmussen, "Suspected Drones Seen over French Military Intelligence Base, Armed Forces Say," *Reuters*, Dec. 09, 2025. [Online]. Available: https://www.reuters.com/world/europe/suspected-drones-seen-over-french-military-intelligence-base-armed-forces-say-2025-12-09/

[144] R. Ruitenberg, "Drones Fly over French Strategic Nuclear Submarine Base, Media Report," *Defense News*, Dec. 05, 2025. [Online]. Available: https://www.defensenews.com/global/europe/2025/12/05/drones-fly-over-french-strategic-nuclear-submarine-base-media-report/

[145] Lorne Cook and Vanessa Gera, "NATO announces a new mission to protect undersea cables in the Baltic Sea region," *AP News*, Jan. 14, 2025. [Online]. Available: https://apnews.com/article/nato-finland-baltic-undersea-cables-b8d351fa018d703fe9dbc50459211e61

[146] North Atlantic Treaty Organization, "NATO Launches 'Eastern Sentry' to Bolster Posture along Eastern Flank," NATO News. [Online]. Available: https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank

[147] Reuters, "Drone Breaches Romanian Airspace during Russian Attack on Neighboring Ukraine," *Reuters*, Sep. 13, 2025. [Online]. Available: https://www.reuters.com/world/drone-breaches-romanian-airspace-during-russian-attack-neighboring-ukraine-2025-09-13/

[148] Andrius Sytas and Gram Slattery, "NATO Member Estonia Says Three Russian Jets Violated Its Airspace," *Reuters*, Sep. 19, 2025. [Online]. Available: https://www.reuters.com/business/aerospace-defense/nato-member-estonia-says-three-russian-jets-violated-its-airspace-2025-09-19/

[149] Andrew Gray, Jacob Grønholt-Pedersen, and Ingrid Melander, "EU Leaders to Discuss 'Drone Wall' in Denmark, Days after Airspace Violations," *Reuters*, Sep. 30, 2025. [Online]. Available: https://www.reuters.com/business/aerospace-defense/eu-leaders-discuss-drone-wall-denmark-days-after-airspace-violations-2025-09-30/

[150] Agence France-Presse, "Berlin Airport Briefly Suspends Operations over Drone Sighting," *CP24*, Mar. 11, 2026. [Online]. Available: https://www.cp24.com/news/world/2026/03/11/berlin-airport-briefly-suspends-operations-over-drone-sighting/

[151] Richards J. Heuer Jr., *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 1999. [Online]. Available: https://www.cia.gov/resources/csi/static/Pyschology-of-Intelligence-Analysis.pdf

[152] Kevin H. Knuth, Robert M. Powell, and Peter A. Reali, "Estimating Flight Characteristics of Anomalous Unidentified Aerial Vehicles," *Entropy*, vol. 21, no. 10, 2019, doi: 10.3390/e21100939.

[153] Norman Fenton and Martin Neil, *Risk Assessment and Decision Analysis with Bayesian Networks*, 2nd ed. Chapman and Hall/CRC, 2018. doi: 10.1201/b21982.

[154] G. K. Haines, "CIA's Role in the Study of UFOs, 1947-90," *Stud. Intell.*, vol. 40, no. 5, pp. 67–84, 1997.

[155] Edward U. Condon and Daniel S. Gillmor, *Final Report of the Scientific Study of Unidentified Flying Objects Conducted by the University of Colorado under Contract to the United States Air Force*. Bantam Books, 1969. [Online]. Available: https://apps.dtic.mil/sti/tr/pdf/AD0680975.pdf

[156] Tim Lomas, Andrew O'Malley, Michael P. Masters, and Rony Vernet, "The UAP Assessment Matrix: A Framework for Evaluating Evidence and Understanding Regarding Unidentified Anomalous Phenomena," *Acta Astronaut.*, vol. 234, pp. 491–503, 2025, doi: 10.1016/j.actaastro.2025.04.012.

[157] Central Intelligence Agency, Center for the Study of Intelligence, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," Central Intelligence Agency, Mar. 2009. [Online]. Available: https://www.cia.gov/resources/csi/static/Tradecraft-Primer-apr09.pdf

[158] G. G. de la Torre, "Psychological Aspects in Unidentified Anomalous Phenomena (UAP) Witnesses," *Int. J. Astrobiol.*, vol. 23, no. e4, 2024, doi: 10.1017/S1473550423000289.

[159] Kevin Cortes, "Pilot Career Consequences for UAP/UFO Reporting," Americans for Safe Aerospace, Dec. 2025. [Online]. Available: https://cdn.sanity.io/files/2469eerl/production/d73e1d5e0e5394151aad6b0dff6a743ad0f002a9.pdf

[160] Kevin Cortes, "Why Don't Pilots Report What They See? Understanding the Career Risks Behind UAP Reporting," Americans for Safe Aerospace. [Online]. Available: https://www.safeaerospace.org/news/why-don-t-pilots-report-what-they-see-understanding-the-career-risks-behind-uap-reporting

[161] NASA Communications, "Artemis II Flight Day 7: Crew Makes Long-Distance Call, Begins Return," NASA Blogs. [Online]. Available: https://www.nasa.gov/blogs/missions/2026/04/07/artemis-ii-flight-day-7-crew-makes-long%E2%80%91distance-call-begins-return/

About the Cover

The cover is a contemporary inversion of Plato's Cave. In the original allegory, prisoners face a wall and mistake puppeteers' shadows for truth. Here, the figure, a "Sensemaker", has already turned, attending with curiosity to anomalous lights entering through fractures in the cave wall.

Suspended above the Sensemaker is the hypothesis space the paper asks its readers to hold open until evidence justifies closure. The five glyphs represent the explanatory categories developed in *Part II: Detect & Identify*: [⊞] sensor artifact (H1), [≋] natural phenomenon (H2), [⊠] familiar human-made technology (H3), [Δ] unrevealed human-made technology (H4), and [✶] genuinely unknown origin (H5). The two marks rising above the cluster (an exclamation and a question) encode the two epistemic states the practice moves between: recognition and inquiry.

The practice the paper argues for is the cultivation of disciplined attention to uncertainty rather than its elimination. The Sensemaker recognizes the unknowns, confronts them, and stays with them. They neither point nor declare nor panic.

The mark worn into the cloth of the Sensemaker's chest is a contemporary echo of the radar-and-interrobang emblem of the Confronting Unknowns program. They are identified by what they practice rather than by who they are. A reader is invited to recognize themselves in the posture.

Attending the Unknown, by Jonathan "JMill" Miller. Charcoal and gouache, digital. May 2026.

Notes

Confronting Unknowns

A framework for anomalous aerospace events

June 2026

https://www.sensemaking.wtf

rev.1.07-20260624-0931_jm