

Left of Launch:

Transforming Counter-UAS Operations with AI-Powered Intelligence

Primer

Date: July 2025

White Paper

Executive Summary

From data overload to decision advantage

The proliferation of Unmanned Aircraft Systems (UAS) presents a complex and escalating threat to national security and public safety. From off-the-shelf drones modified for malicious use to sophisticated state-sponsored platforms, these systems are used for everything from surveillance and smuggling to kinetic attacks. Government agencies tasked with confronting these systems are inundated with disconnected data from sensors, field reports, and public sources, overwhelming traditional methods for analysis and planning.

Focus needs to shift from simple detection to proactive, predictive intelligence. This paper outlines how Primer's AI-powered platform can give government agencies the upper hand. By fusing proprietary and open-source intelligence (OSINT), can create a unified view of the threat landscape, expose hidden networks, and dispatch real-time alerts to teams in the field.

By leveraging advanced AI to read, understand, and connect information locked in unstructured data, noise turns into actionable insight. The takeaway is a fundamental shift in the counter-UAS mission: empowering agencies to operate "left of launch," staying ahead of evolving threats and pivoting to a proactive defense posture with speed and precision.

National strategy alignment

This AI-enabled approach directly supports U.S. federal counter-UAS strategy. It aligns with the DoD's December 2024 National Strategy for Countering Unmanned Systems and the DHS Domestic C-UAS Action Plan, both of which emphasize proactive threat detection, data fusion, and cross-agency coordination. Primer's technology helps operationalize these priorities and aims to enhance situational awareness and enable faster, intelligence-driven decision cycles.

©2025 Primer

The Problem: A Sky Full of Unknowns

Understanding the modern, asymmetric drone threat

Safeguarding a nation's people, values, and homeland has entered a new dimension. Airspace has become an operational front, with a rapidly growing and increasingly complex threat from unauthorized, modified, or malicious UAS. They are no longer theoretical concerns; they are actively used for hostile surveillance, intelligence collection, cross-border smuggling of narcotics and weapons, and potential attacks against critical infrastructure and the public.

Small, low-signature, fast-moving, and increasingly autonomous drones have become so affordable and accessible that state and non-state actors can field them at scale, overwhelming traditional defenses and exposing critical gaps in early threat detection and response.

The Intelligence Challenge

Why traditional methods can't keep pace

Across government, personnel tasked with the counter-UAS mission struggle for coherent insight, constrained by critical limitations:

- **Data overload:** The torrent of drone-related data is swamping manual review. Analysts must to triage internal incident logs, raw sensor streams, classified briefs, and a relentless flood of open-source intelligence — where key clues are often diluted, commingled, or just lost in the noise.
- **Data silos:** Intelligence gathered by federal, state, and local entities often remains in disconnected systems or separate formats that stymie coordination across jurisdictions.
- **Manual processes:** Analysts rely on manual workflows to aggregate and interpret data. The approach is inefficient and prone to miss the subtle connections and emerging threat patterns hidden in the noise. That leaves vital open-source intelligence like news and social media on the table, under-leveraged by busy teams.

These limitations result in blind spots, delayed responses, and a fragmented reactive posture to high-consequence threats near sensitive facilities, active borders and public spaces.

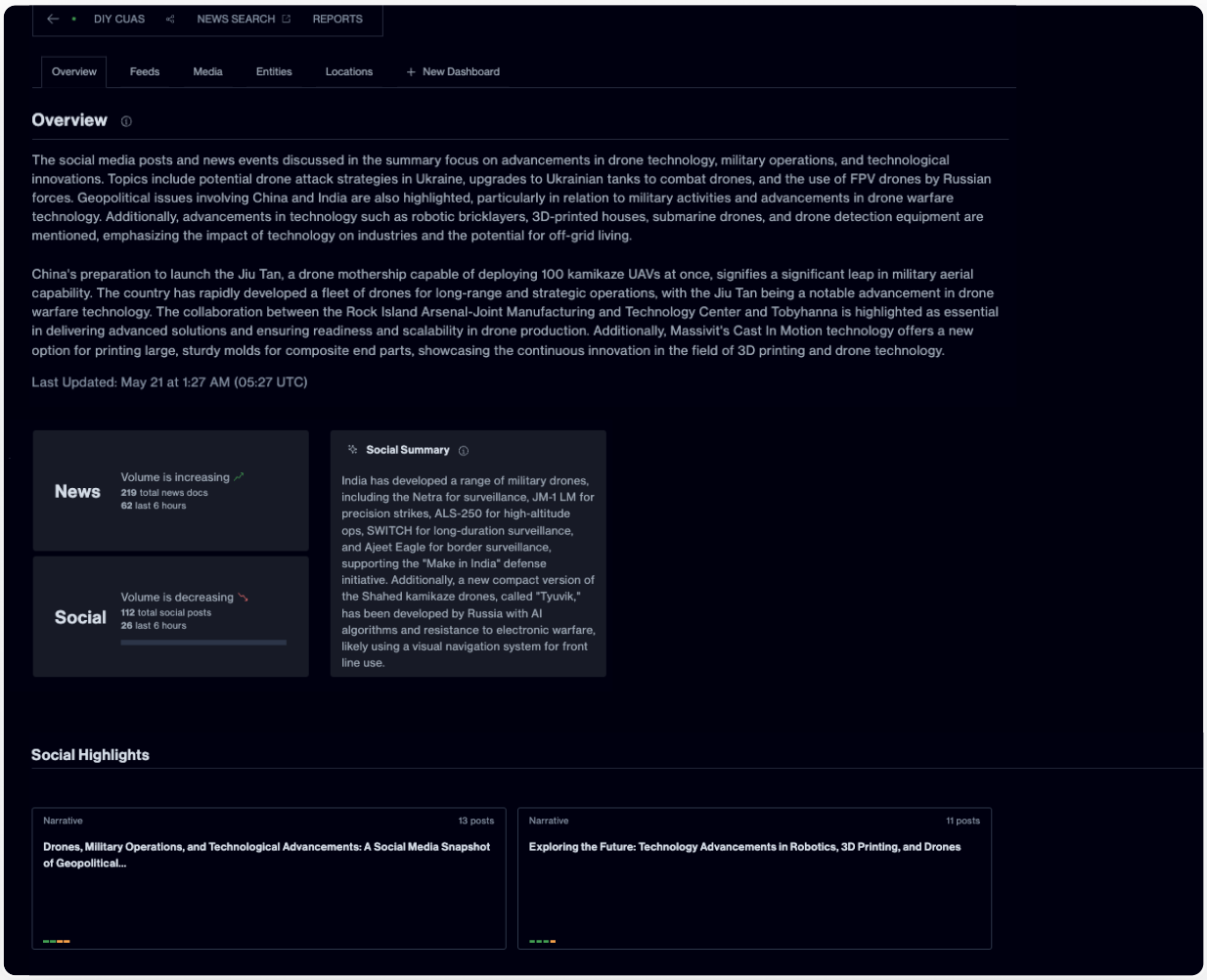
The AI-Enabled Solution

AI that reads, understands, and enables at scale

To get left of launch, agencies must make sense of all their data, automatically and at scale. That requires deploying an advanced AI platform to ingest, filter, structure, and analyze the vast majority of intelligence locked away in unstructured text, an estimated 80-90% of all data across the enterprise.

Explaining the technology:

- **Natural Language Processing (NLP):** At its core, this is AI that reads and understands human language, scans millions of documents (from formal government reports to social media posts) in seconds, identifying and extracting critical details: drone models, tactics techniques and procedures (TTPs), locations, and associated individuals.
- **Data Fusion:** The platform automatically connects related information from disconnected sources. It can integrate internal incident reports, sensor logs, and other proprietary data with open-source intelligence from around the world to create a single, coherent picture of the information landscape, ready for targeted queries.
- **Trust and Verification (RAG-V):** Trust is non-negotiable, so Primer uses Retrieval-Augmented Generation with Verification (RAG-V), a system designed to boost AI reliability by breaking down individual claims and validating against the original source documents. Every piece of insight links back to the source material with footnote-level traceability, cutting hallucination rates in half compared to other state-of-the-art systems and giving every user the power to instantly verify all information.
- **Complementing Traditional Counter-UAS:** While most counter-UAS platforms focus on detecting or disabling drones after launch (assisted by sensors, radars, or kinetic tools), Primer operates earlier in the threat chain. From vast volumes of data, Primer surfaces pre-launch indicators, identifies emerging TTPs, and flags adversarial narratives that often precede incursions.



Primer real-time OSINT collection of evolving DIY Drone TTPs collected from news and social media

Core Capabilities

Translating technology into tangible mission outcomes

AI turns raw data into instant insight — flagging threats, mapping networks, and issuing SITREPs — so analysts, operators, and commanders can act decisively.



Primer AI's Geo driven intelligence, transforming unstructured CUAS data into actionable insights

- **Instantly spot critical details.** The platform automatically extracts key details buried in raw text: people, locations, device serial numbers, RF protocols, pilot behavior, and more – surfacing threats before they even coalesce.
- **Uncover hidden networks and timelines.** Fusing fragmented data lets the AI build coherent timelines and narratives of events. Changes over time reveal evolving TTPs, networks of operations, and patterns of action that would never emerge from manual review.
- **Generate automated situational reports.** Analysts can receive automated daily situational reports (SITREPs) with concise, field-ready summaries of developments in real time.
- **Run on classified or unclassified networks.** Primer is accredited and deployed on JWICS, NIPRNet and secure commercial cloud, offering identical analytic workflows and data-provenance controls across security domains.

Mission Impact Across the Public Sector

AI that amplifies every operation

AI-powered counter-UAS acts as a force multiplier across a range of government missions.

- **Protecting critical infrastructure:** Detect emerging surveillance or proximity-based threats targeting energy facilities, airports, government buildings, and other restricted zones to prioritize and triage the response.
- **Combating transnational crime:** Identify the patterns of drone incursions, whether for narcotics, weapons, or human smuggling, even when the platforms are DIY, unregistered, or modified to elude detection.
- **Strengthening border security:** Give field agents real-time alerts and localized threat summaries by fusing data on drone sightings, pilot telemetry, and cross jurisdiction incident data.
- **Securing public safety:** Proactively monitor and flag drone behavior that suggests pre-op planning or hostile surveillance near public gatherings, providing security teams with critical lead time to intervene.
- **Securing high-profile public events:** Surface and assess drone activity around major gatherings, such as national ceremonies, sporting events, and global summits, to help enable timely interventions.
- **Supporting emergency response and disaster relief:** Monitor drone activity in disaster zones or restricted airspace to ensure safe operations among first responders, humanitarian teams, and federal agencies.

Conclusion: Building a Proactive Defense Posture

The future of counter-UAS is proactive, not reactive

The UAS threat is evolving too quickly for yesterday's methods, and reacting to drone incursions that are already underway just won't suffice. True security means building and maintaining a wide-angle, real-time understanding of the entire threat landscape.

An AI-centric approach allows government agencies to fuse data across sources, automate complex analysis, and deliver verified, actionable intelligence to the people who need it most. This technology will advance counter-UAS operations from a reactive "detect and respond" model to a proactive strategy focused on understanding, anticipating, and neutralizing threats. It can be a force multiplier that empowers organizations and agencies to protect the nation's airspace and safeguard critical assets with agility, precision, and confidence.

We build decision-ready AI for the world's most critical organizations.

Contact us at **publicsector@primer.ai**

Learn more: www.primer.ai

©2025 Primer