

UNMANNED UNITED INC.

Threat Analysis of a Long-Range Autonomous Unmanned Aerial System

A public position paper from an American autonomous-systems company

Long-range autonomous unmanned aerial systems are changing the security problem faster than traditional perimeter, air-defense, and response models were designed to adapt. Their threat is not defined by a single airframe or payload. It is the combination of distance, persistence, low operating cost, distributed control, and the ability to impose uncertainty on defenders.

UNMANNED UNITED POSITION

The United States should treat long-range autonomy as a systems-security challenge: detect earlier, classify better, preserve decision time, harden critical infrastructure, and maintain a trusted domestic industrial base able to iterate at the pace of the threat.

The Threat Is a System, Not a Platform

THREAT ATTRIBUTE	WHY IT MATTERS	DEFENDER'S DESIGN QUESTION
Range and persistence	A small autonomous system can observe, relay information, or approach from beyond the immediate security footprint.	How does the force create awareness before the final approach?
Distributed control and autonomy	A system may remain effective despite intermittent links or remote operators.	How do teams plan for degraded communications and rapid changes in behavior?
Low-cost iteration	Commercial components and rapid manufacture shorten adversary learning cycles.	How do acquisition and testing cycles keep pace without sacrificing assurance?
Multi-domain effects	Aerial observation, RF activity, logistics, and information operations can be mutually reinforcing.	How are sensors, operators, and response authorities connected into one picture?

A USA-First Response

A durable response must be more than a procurement preference. It requires domestic design authority, transparent supply chains, trusted software and data handling, repairable systems, and the ability to modify platforms as missions evolve. The objective is not simply to buy aircraft; it is to preserve the freedom to inspect, adapt, sustain, and improve the systems that protect American personnel and infrastructure.

- Invest in and Prioritize American-controlled design, software, data, and supply-chain visibility.
- Use layered sensing: visual, thermal, RF-awareness, radar, and human reporting—each with clear confidence limits.
- Make the human decision-maker the center of the system, not the last recipient of disconnected feeds.
- Invest in persistent, modular airborne platforms that can carry evolving sensor and communications mission kits.
- Design for sustainment from the beginning: spares, training, software updates, diagnostics, and configuration control.

Implications for Autonomy

Autonomy should increase operator capacity, not obscure accountability. The most useful systems reduce search burden, present evidence with provenance, maintain communications resilience, and support deliberate human decisions. Effective deployment therefore depends on practical integration: trained crews, defined rules, trustworthy interfaces, and common operating pictures that make uncertainty visible rather than hiding it.

Questions for Government and Industry

- What threat indicators must be detected outside the protected perimeter—and which authority is responsible for acting on them?
- What data must remain U.S.-controlled throughout the platform lifecycle?
- How quickly can a new payload, software release, or mission configuration be verified and fielded?
- What constitutes usable evidence for an operator facing uncertain or time-sensitive aerial activity?

UNMANNED UNITED | AMERICAN-BUILT AUTONOMY

Learn more or start a mission discussion: www.unmannedunited.com | sales@unmannedunited.com

Public discussion document. This paper describes general operational considerations and does not disclose Unmanned United proprietary designs, methods, performance data, operational tactics, or controlled technical information. Nothing herein is an offer to provide a weapon system, a technical manual, or operational advice.