Robotic Warfare and Defense As A Service

An Operational Thesis for Robotic Defense

Colony Dynamics Inc.
United States

May 2026

Abstract

This paper states Colony's thesis for robotic warfare and Defense As A Service. Robotic warfare is not defined by a single autonomous weapon. It is the use of distributed uncrewed systems to sense, maneuver, coordinate, and apply effects across air, land, surface, and subsurface domains. These systems turn combat power into a problem of networks, availability, production, and software. Defense As A Service is the operating model that follows from that change. The customer purchases a continuously available defensive outcome rather than individual systems and the burden of operating them. The provider carries readiness risk across the full system. The customer retains command, policy, rules of engagement, and use-of-force authority.

1 Robotic Warfare

Robotic warfare is combat in which distributed uncrewed systems perform sensing, maneuver, coordination, and effects under human command. The relevant measures are network speed, availability, scale, adaptability, and regeneration.

The definition is broader than "autonomous weapons." It includes teleoperated, automated, semi-autonomous, and autonomous systems. It also includes the people, sensors, software, communications, logistics, and rules of engagement that allow those systems to operate. A robot is one node in the force. The network is the weapon. Autonomy defines how much independence a machine has for a specific task. Human command defines the objective, limits, authority, and accountability for that task.

The transition is already visible. The U.S. Department of Defense created Replicator to accelerate the fielding of thousands of all-domain attritable autonomous systems. Scale, software, and production speed are now operational requirements [1]. Ukraine reported 8,150 Shahed, Gerbera, Italmas, and related UAV launches in May 2026 and 7,476 interceptions [2]. Its Ministry of Defence also reported combat-tested interceptors that automate 95 percent of the interception cycle after an operator selects and authorizes the target [3]. NATO defines integrated air and missile defense as a continuous, networked, layered activity [4]. Joint Interagency Task Force 401 states the same problem directly: drones are systems, and protection is an outcome rather than a single engagement [5].

These facts change the procurement question. The relevant question is no longer, "What is the best drone?" It is: what network can repeatedly convert warning into an authorized effect, confirm the result, restore readiness, and do it again before the next attack? A fleet that has been purchased but is not available is not combat power.

2 The Laws of Robotic Warfare

1. **The network is the weapon.** Platform performance matters only when sensing, communications, command, effectors, operators, and sustainment work as one system. The best component cannot compensate for a broken chain.
2. **Availability is combat power.** The force exists only when enough systems, effectors, people, links, spares, and maintenance capacity are ready at the same time. The Government Accountability Office reports that operating and support costs account for roughly 70 percent of weapon-system cost and continues to document readiness and sustainment shortfalls [6].
3. **The campaign matters more than the unit price.** Purchase price is an incomplete measure. The relevant measures are cost per protected hour, cost per confirmed effect, magazine regeneration, expected leakage, and the cost of a successful attack on the defended asset. A cheap robotic attack can impose a strategic loss.
4. **Humans command; machines execute at machine speed.** Humans define intent, protected objects, constraints, and authorization. Machines can classify, allocate, navigate, coordinate, and complete bounded tasks. DoD Directive 3000.09 requires appropriate human judgment over the use of force and realistic verification and validation of autonomous functions [7].
5. **Regeneration is part of the weapon.** A system that cannot be rearmed, repaired, replaced, or retasked at campaign tempo is a demonstration asset. Reserves, common interfaces, field maintenance, replenishment, and degraded operation belong inside the combat architecture.
6. **Operational data is part of the force.** Every deployment should improve models, software, tactics, maintenance intervals, force allocation, and cost estimates. A force that learns from every operation can adapt faster than a platform-centered acquisition cycle.

3 Defense as a Service

Defense As A Service is a performance-based operating model in which a provider delivers a defined defensive outcome and carries readiness risk across hardware, software, personnel, maintenance, logistics, replenishment, and continuous improvement. The customer retains sovereign command, policy, rules of engagement, and use-of-force authority. Colony carries readiness risk. The customer retains sovereign authority [11].

The product is not a number of aircraft, sensors, or interceptors. It is an available defensive posture over a defined geography and threat class. The provider is responsible for fleet availability, trained operators and maintainers, mission software, customer integration, spares, repairs, replenishment, configuration control, event logs, performance reporting, and restoration after failure. The government defines protected priorities, operational command, legal authority, rules of engagement, intelligence boundaries, acceptance criteria, audit rights, and remedies.

3.1 Government Authority

Defense As A Service does not transfer command of military forces to a contractor. Federal Acquisition Regulation Part 37 directs agencies to use performance-based acquisition for services to the maximum extent practicable [8]. FAR Subpart 7.5 reserves inherently governmental functions, including command of military forces, to government personnel [9]. The intended model is a contractor-owned or contractor-operated defensive capability under government command. The provider operates and sustains the service. The government decides when and how force may be used.

3.2 The Contract Unit

The correct contract unit is an operated defended sector or mission envelope. At minimum, the contract must specify:

- protected geography, mission, and threat class;
- availability by time, weather, and threat state;
- detection-to-action and restoration-time distributions;
- ready magazine, surge capacity, and replenishment obligations;
- confirmed outcome rate with uncertainty and denominator reporting;
- cost per protected hour and per confirmed effect;
- customer-provided sensor, command-and-control, and authority assumptions; and
- audit rights, data rights, remedies, and transition or exit conditions.

This service definition controls the engineering. Endurance matters because it changes sortie generation. Maintainability matters because it changes availability. Manufacturing matters because attrition and spares determine whether the service continues. Software matters because the threat adapts. Every component is judged by its contribution to the contracted outcome.

4 The Standard of Proof

A Defense As A Service claim is valid only when the provider measures the full operating chain. Terminal performance, a successful demonstration, or a platform specification cannot substitute for deployed performance. The basic system probability is

$$P_{\text{defeat}} = P_{\text{track}} P_{\text{class}} P_{\text{auth}} P_{\text{allocate}} P_{\text{launch}} P_{\text{acquire}} P_{\text{effect}}. \tag{1}$$

This equation does not assume that the terms are statistically independent. A single failure can affect several terms. The point is to prevent a provider from reporting terminal interceptor performance as if it were system performance. Each term must be measured separately. The full result must include the operating conditions, denominator, and uncertainty.

Evidence must distinguish measured results, design targets, modeling assumptions, public evidence, and scope boundaries. Results must be separated by weather, visibility, target state, sensor source, communications state, operating tempo, hardware age, authorization state, and any other condition that changes performance. A provider that guarantees an outcome must state what has been measured and what remains an assumption.

5 Governance and Accountability

Human authority is part of the system architecture. Machine behavior must be tied to a human-authorized objective, defined target classes, time and geographic limits, realistic verification and validation, traceable logs, intervention or deactivation mechanisms, and a named chain of accountability. DoD policy requires appropriate human judgment and realistic testing [7]. The International Committee of the Red Cross warns that loss of human control creates legal, ethical, and humanitarian risk [10].

The design objective is not to remove the human. It is to place human judgment at the level of intent, authorization, and accountability while machines handle tasks that require speed, persistence, and scale. Clear authority reduces hesitation, limits the machine to the approved mission, and makes every action auditable.

6 Conclusion

Robotic warfare changes what a military must buy and operate. Individual platform performance still matters, but it is not the final product. The final product is a network that can convert warning into authorized action, absorb failures and attrition, restore readiness, and improve as the threat changes.

The win condition is not a better drone. It is a defensible service-level proposition: the provider can keep a defined area protected against a defined robotic threat at an economically favorable cost, while the customer avoids building the organization required to operate that defense itself. The claim fails if terminal performance, integration, availability, attrition, replenishment, or sustainment prevent the provider from meeting the contract. The customer should buy defended operations, measure the full system, retain sovereign authority, and hold the provider responsible for readiness.

References

[1] U.S. Department of Defense, "Replicator All-Domain Attritable Autonomous Systems," releases of 6 May and 13 November 2024. Defense.gov.

[2] Ministry of Defence of Ukraine, "Ukrainian Air Defense Intercepted Nearly 92% of Drones Amid Intensified Aerial Attacks in May," 5 June 2026. Ministry of Defence of Ukraine.

[3] Ministry of Defence of Ukraine, "Next-Generation Interceptors: Ukrainian Drones Already Autonomously Take Down Shahed-Type UAVs," 8 June 2026. Ministry of Defence of Ukraine.

[4] North Atlantic Treaty Organization, *NATO Integrated Air and Missile Defence Policy*, 13 February 2025. NATO.

[5] Joint Interagency Task Force 401, *Small Drones, Big Problems: A First Principles Approach to Countering-UAS*, 18 June 2026. U.S. Department of Defense.

[6] U.S. Government Accountability Office, *Weapon System Sustainment*, GAO-24-107378, 29 February 2024. GAO.

[7] U.S. Department of Defense, *DoD Directive 3000.09: Autonomy in Weapon Systems*, 25 January 2023. U.S. Department of Defense.

[8] Federal Acquisition Regulation, Part 37, "Service Contracting." Acquisition.gov.

[9] Federal Acquisition Regulation, Subpart 7.5, "Inherently Governmental Functions." Acquisition.gov.

[10] International Committee of the Red Cross, "ICRC Position on Autonomous Weapon Systems," 12 May 2021. ICRC.

[11] Colony Dynamics Inc., *Defense As A Service: An Operational, Technical, and Economic Thesis for Persistent Counter-Shahed Protection*, May 2026.