Intelligence Preparation of the Battlefield

in the Era of UAS: Adapting ATP 2-01.3 to the Transparent Battlefield, the Reconnaissance-Strike Complex, and Left-of-Launch Intelligence

ASSESSMENT SCOPE

This paper examines how the mass employment of UAS in large-scale combat operations has fundamentally altered each of the four IPB steps codified in ATP 2-01.3. It addresses what the transparent battlefield means for step 1 (defining the operational environment), how drone-driven kill-zone deepening reshapes step 2 (environmental effects), how the reconnaissance-strike complex and AI-enabled autonomous systems transform step 3 (threat evaluation), and how fiber-optic, EW-resistant, and swarm threats change step 4 (threat courses of action). It proposes a UAS-integrated IPB framework structured around six analytical disciplines not addressed in current doctrine, and identifies the doctrinal and training changes required to execute IPB that matches the pace and precision of the modern drone threat.

PRIMARY SOURCES

ATP 2-01.3 IPB (Mar 2019) | FM 2-01.3/MCRP 2-3A IPB (2009) | FM 3-01.7 Appendix B Aerial IPB | FM 2-0 Intelligence (active revision Mar 2026) | FM 3-0 Operations (Mar 2025) | ATP 3-01.81 C-UAS (Aug 2023/May 2025) | CEPA: An Urgent Matter of Drones (2025) | ICDS: Fortification for Drone Warfare (Oct 2025) | CSIS: Lessons from Ukraine, Modern Warfare in the Age of Autonomy (May 2025) | CSIS: Ukraine AI-Enabled Autonomous Warfare (Mar 2025) | MWI: Battlefield Drones and the Autonomous Arms Race (Jan 2025) | SWJ: The New Arms Race (Dec 2025) | Defence Ukraine: FPV Drones in the Ukraine War (Aug 2025) | TRADOC G2 OE: Ukrainian UAS Tactics (Oct 2024) | Army.mil: Drone Dominance Doctrine Update (Mar 2026) | Inside Unmanned Systems: Army Rewrites Drone Doctrine (Apr 2026) | Military Review 2024: MG Vowell/MAJ Padalino | CRS R48477 (Mar 2025)

April 2026 | UNCLASSIFIED

This paper draws exclusively on publicly available and officially released sources. No classified information is referenced.

Executive Summary

Intelligence Preparation of the Battlefield is the analytical engine of the military planning process. ATP 2-01.3 defines IPB as the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. That definition was built around a threat environment in which air threats were manned aircraft, ballistic missiles, and cruise missiles, and in which the primary intelligence challenge was to understand how an adversary with known doctrine, identified order of battle, and observable logistics would move through predictable terrain toward identifiable objectives.

The UAS threat environment of 2024-2026 fits that analytical model in almost no dimension. Small commercial and military-grade drones costing hundreds to thousands of dollars are produced at industrial scale, with Ukraine manufacturing approximately 2 million drones in 2024, of which 96.2 percent were domestically produced. They operate below the radar floor of most organic air defense sensors, navigate GPS-denied environments using inertial guidance and optical flow, resist electronic warfare through frequency-hopping and fiber-optic tethering, and strike with accuracy that previously required precision-guided munitions. The reconnaissance-strike complex, in which a UAS identifies a target and passes targeting data to artillery or a strike drone, has compressed the sensor-to-shooter timeline to under two minutes in documented Ukrainian engagements. A single drone operator with a commercially available quadcopter and a modified munitions drop system can render a command post non-mission-capable faster than the S-2 section it serves can complete a named area of interest analysis.

The consequences for IPB are structural, not incremental. Each of the four steps requires modification. Defining the operational environment now requires mapping the drone-accessible airspace as terrain, identifying commercial and military UAS launch areas, and assessing the electromagnetic spectrum as both a threat indicator and a friendly vulnerability. Describing environmental effects requires understanding how drone saturation reshapes maneuver, logistics, command post siting, and signature management across the full operational depth. Evaluating the threat requires moving beyond platform identification to network analysis: who operates the drones, where are operators positioned, what are their shift patterns, how are drones charged and recovered, and what is the decision cycle between drone observation and artillery effect. Determining threat courses of action requires templating not just where enemy forces will maneuver but where their UAS will operate, what sensor coverage they will provide, and how the RSC will translate that coverage into fires effects against friendly targets.

THE SIX IPB GAPS THE UAS ERA CREATES

Gap 1: Volume and dispersal. Current IPB frameworks were designed for platforms with identifiable launch sites and fixed order of battle. UAS are produced in platoon-sized quantities and launched from any flat surface. No current IPB template accounts for this threat density or dispersal.

Gap 2: The transparent battlefield. FM 3-0 March 2025 introduces 'protect against constant observation' as an operational imperative. ATP 2-01.3 Step 2 has no analytical framework that treats persistent aerial surveillance as an environmental constant rather than an episodic event.

Gap 3: Kill zone deepening. The ICDS fortification analysis documents a kill zone deepened to 35-40 km and a safe rear that has largely vanished. IPB terrain products and named areas of interest have not been restructured to reflect this expanded danger zone.

Gap 4: The reconnaissance-strike complex. The RSC integrates UAS observation with fires in a single kill chain. ATP 2-01.3 addresses air threats and fires threats in separate steps. No current IPB framework treats the RSC as a unified analytical object.

Gap 5: Left-of-launch intelligence. Ukrainian experience shows that disrupting UAS capability requires targeting drone operators, shift schedules, charging infrastructure, and supply chains. Current IPB high-value target development does not systematically address the human and logistics network behind drone employment.

Gap 6: AI-enabled autonomy. Ukraine conducted its first fully unmanned combat operation in December 2024. AI-enabled target recognition is in active production. IPB has no framework for evaluating a drone threat that does not require a human operator for targeting or engagement.

1. The IPB Doctrinal Baseline and Its UAS-Era Limitations

1.1 ATP 2-01.3 and the Four-Step Framework

ATP 2-01.3, the Army's current IPB authority, defines a four-step process: defining the operational environment, describing environmental effects, evaluating the threat, and determining threat courses of action. As a dual-designated Army and Marine Corps publication it represents the joint-service standard for tactical IPB. The G-2 and S-2 hold staff proponency for IPB, though the manual emphasizes that every commander and every member of the staff needs to understand and apply IPB during the staff planning process.

For air threats, FM 3-01.7 Appendix B provides the Aerial IPB analytical template. It identifies the most significant aerial threats as UAVs, ballistic missiles, cruise missiles, and fixed- and rotary-wing aircraft, and frames the air area of operations as extending to the maximum range of aircraft and missiles plus threat airfields, forward arming and refueling points, navigation aids, and missile sites. Analysis begins at the threat airfield or UAV launch site and works toward probable enemy objectives. The framework correctly notes that ground corridors do not limit missiles and ISR UAVs. This structure was sound for its designed threat environment but was written before small commercial UAS became the primary tactical reconnaissance and strike platform at the company and platoon level.

The March 2026 Army doctrine overhaul confirms that FM 2-0, Intelligence, is being updated to expand sections on adversary UAS capabilities and individual Soldier tasks related to the drone threat. The Inside Unmanned Systems April 2026 reporting on the Army's drone dominance doctrine initiative identifies FM 2-0 as a foundational manual currently undergoing UAS-specific revision. These revisions are in progress. The analytical framework they need to incorporate is examined in the following sections.

1.2 What the Current Framework Cannot Produce

The gap between what ATP 2-01.3 is designed to produce and what the UAS threat environment requires is specific and bounded. IPB Step 3, Evaluate the Threat, produces threat order of battle, doctrinal templates, and high-value target lists keyed to platform identification and force structure analysis. The modern drone threat requires instead a network analysis product mapping drone operators, charging teams, reconnaissance

relay personnel, targeting analysts, and supply chain nodes as a human network threat, analogous to the targeting approach JIEDDO developed for IED networks during the Global War on Terror.

IPB Step 4, Determine Threat Courses of Action, produces threat event and situation templates describing where threat forces will move and when. The UAS threat requires instead a sensor coverage template: a geospatial product mapping the electromagnetic and optical coverage that threat UAS will provide across the friendly area of operations, identifying areas of persistent surveillance, detection ranges for specific UAS sensor payloads against specific friendly signature types, and the correlation between UAS observation events and subsequent fires effects. This sensor coverage template does not exist as a standard IPB product in ATP 2-01.3.

Military Review 2024 documented the assessment by then-Major General Joel B. Vowell and Major Anthony R. Padalino that existing mission command systems fielded to counter enemy UAS lack the necessary technological capabilities to adequately defend combat power on today's battlefield, and that C-UAS mission command systems require artificial intelligence, machine learning, and automation to assist operator decision-making. The IPB framework that feeds those mission command systems has the same deficit. It cannot currently produce the sensor coverage template, the network analysis product, or the RSC threat template that effective C-UAS employment requires. The intelligence failure is upstream of the mission command failure.

2. Step 1 Revised: Defining the Operational Environment for Drone Saturation

2.1 The Transparent Battlefield as an Environmental Constant

ATP 2-01.3 Step 1 identifies the limits of the area of operations, the area of interest, and the significant characteristics requiring analysis. In the UAS era, the most operationally significant characteristic is not terrain in the traditional sense but the low-altitude airspace below 400 feet and the electromagnetic spectrum as a domain of persistent threat observation. A British Army General, quoted in CEPA's comprehensive drone analysis, stated precisely what this means operationally: the use of unmanned aerial systems has created a transparent battlefield where there is no sanctuary.

The operational implication for IPB Step 1 is that the area of interest for UAS threat analysis extends not from identifiable threat positions outward but from any position within the threat's drone operating radius inward to every friendly element's position. Ukraine's experience documents that the concept of a safe rear 10-15 km from the contact line has largely vanished and that the kill zone has deepened to 35-40 km, as analyzed by the ICDS fortification study. The FM 3-0 March 2025 revision, adding 'protect against constant observation' as a core operational imperative, confirms that the transparent battlefield is the current operational standard rather than a future threat projection.

Step 1 in the UAS era must include a UAS Operational Environment Definition product that maps: the threat's assessed drone operating radius by platform group; the low-altitude airspace available to threat UAS across the full depth of the area of operations; identified launch areas including forward assembly areas and covered positions with line-of-sight to the friendly area; the electromagnetic spectrum with identified frequencies used

by threat UAS control systems; and terrain features that limit or extend drone operating range, including vegetation, structures, and weather patterns that affect acoustic and optical detection. This product is a UAS-specific annex to the existing Step 1 output, not a replacement for it.

2.2 Signature Management as a Step 1 Intelligence Product

The transparent battlefield transforms signature management from a force protection discipline into an intelligence requirement. The S-2's ability to accurately assess the threat's sensor capabilities, particularly the EO-IR and optical payloads carried by Group 1-3 UAS, is directly relevant to determining which friendly signatures are detectable at which ranges under which conditions. ATP 3-01.81 identifies UAS situational awareness as providing an aerial view that allows the enemy commander to adjust operational orders based on real-time intelligence. Assessing which friendly activities create detectable signatures from drone altitude, and at what ranges under what illumination and atmospheric conditions, is a doctrinal IPB function that the current Step 1 product set does not specify.

3. Step 2 Revised: Environmental Effects in the Drone-Saturated Battlespace

3.1 Terrain and Weather Through the Lens of Drone Employment

ATP 2-01.3 Step 2 describes how terrain and weather affect friendly and threat operations. The Aerial IPB appendix notes that terrain analysis for air and missile defense differs from ground terrain analysis. For Group 1-3 UAS operating below 400 feet, terrain channeling effects are more pronounced than for manned aircraft. A quadcopter in rolling terrain with 20-30 meter vegetation cover has fundamentally different detection geometry than one over open ground. Building density in urban terrain creates dead zones in UAS sensor coverage and limits effective RF control range. The JMRC Skynet Platoon's published experience at Hohenfels notes that RF propagation in that terrain makes it very difficult for ground control stations to push the ranges on those platforms, a terrain effect with direct IPB implications for identifying the boundaries of threat drone employment.

Weather effects on small UAS differ from effects on manned aircraft in ways relevant to Step 2. Wind speed thresholds that ground a fixed-wing aircraft may have negligible effect on a fiber-optic FPV drone below 50 meters. Precipitation affects acoustic signature differently at different UAS altitudes. Fog and low cloud that degrade EO-IR payloads may actually increase UAS effectiveness if threat operators shift to acoustic sensors, while simultaneously degrading visual-based friendly C-UAS response. Step 2 weather analysis for UAS must address: wind speed by altitude band and its effect on each UAS group; precipitation effects on EO-IR sensor performance; fog and low-cloud effects on different sensor modalities; and temperature and humidity effects on battery endurance.

3.2 The Electromagnetic Environment as Terrain

The electromagnetic environment is the most consequential environmental factor for UAS operations and C-UAS response, and it receives no systematic treatment as an environmental element in current ATP 2-01.3 Step 2. RF-controlled drones depend on uncontested spectrum access for command and control, video

downlink, and GPS navigation. EW-capable formations that can deny or degrade those frequencies create an electromagnetic terrain feature that affects where and how threat UAS can operate as profoundly as physical terrain affects ground maneuver.

The CSIS Ukraine analysis confirms that GPS jamming proved particularly effective against systems relying on GPS for navigation, forcing Ukrainian operators to develop inertial navigation and line-of-sight communications as alternatives. The evolution of fiber-optic FPV drones, documented by Defence Ukraine, is a direct operational response: fiber-optic control eliminates the RF signature and renders the drone completely immune to jamming and undetectable by RF direction-finders. For IPB Step 2, the electromagnetic terrain map must identify: friendly and threat EW emitter positions and their effective jamming ranges by frequency band; GPS-denied zones and their boundaries; RF-congested areas where drone control signal quality degrades; and terrain features affecting RF propagation.

4. Step 3 Revised: Evaluating the UAS Threat

4.1 Beyond Platform Identification: The Drone Operator Network

ATP 2-01.3 Step 3, Evaluate the Threat, produces an assessment of threat characteristics, order of battle, doctrine, tactics, and behavior. For conventional threats, this analysis is anchored to identified units with known equipment, established doctrine, and observable logistics. The UAS threat requires a fundamentally different analytical approach because the operationally relevant threat is not the drone in flight but the human-machine network behind it.

The Small Wars Journal analysis of Ukraine's UAS ecosystem identifies precisely what this network consists of: drone operators, relay personnel extending control range using airborne repeaters, reconnaissance analysts processing the video feed and identifying targets, fires integration personnel translating UAS targeting data into artillery or strike drone tasking, recovery and maintenance teams, and supply chain nodes providing batteries, replacement components, and airframes. Ukrainian battlefield awareness improvements have focused on targeting pilot pipelines specifically, including predictions of Russian pilot shift changes to time movements and attacks. This shift-change targeting model represents left-of-launch intelligence at the tactical level: the S-2 is not analyzing where drones will fly but when operators rotate, enabling maneuver windows when drone threat density is lowest.

Step 3 in the UAS era must produce a UAS Threat Network Analysis product analogous to the network analysis developed for IED networks during the Global War on Terror. This product maps: identified drone operator teams by assessed location and shift schedule; charging and recovery infrastructure; relay and retransmission positions; reconnaissance-to-fires integration nodes; supply chain routes and resupply frequency; command relationships governing drone employment authority; and assessed proficiency by unit. Each network node is a potential high-value target. The shift schedule assessment is the analytical product that enables the left-of-launch maneuver window that Ukrainian forces learned to exploit.

Exhibit 1 | UAS Threat Evaluation: Current ATP 2-01.3 Approach vs. Required UAS-Era Extension

Step 3 Element	Current ATP 2-01.3 Approach	UAS-Era Extension Required
Order of Battle	Unit identification, equipment, strength, disposition by echelon	UAS operator teams, drone inventory by group, charging/recovery infrastructure, relay network, assessed crew proficiency
Doctrine and TTPs	Reference published doctrine; compare observed behavior to doctrine	Analyze observed UAS employment patterns: shift schedules, relay architecture, RSC integration sequence, EW adaptation TTPs, fiber-optic vs. RF control selection criteria
High-Value Target List	Platforms, C2 nodes, logistics, key leaders by echelon	Drone operators by proficiency, charging infrastructure, relay aircraft, ground control stations, RSC fires integration nodes, component supply routes
Threat Indicators	Order of battle changes, logistics activity, signal activity, engineering	Drone acoustic signatures, RF emission patterns, operator position activity, visual staging of drone equipment, relay aircraft launch, RSC activation sequence
Threat Capability Assessment	Platform ranges, weapons effects, maneuver speed, sustainment rates	UAS sensor payload capability, detection ranges vs. friendly signature types, EW resistance by control method, autonomy level, swarm coordination capability
AI/Autonomous Systems	Not addressed in current doctrine	AI-enabled target recognition capability, GPS-independence through optical flow or inertial navigation, swarm coordination algorithms, autonomous engagement authority level

4.2 The Reconnaissance-Strike Complex as a Unified Analytical Object

The reconnaissance-strike complex is the defining analytical challenge of UAS-era IPB Step 3. The CSIS analysis of Ukraine's AI-enabled autonomous warfare describes the RSC precisely: the kill chain merges reconnaissance and strike UAVs with artillery in a unified command system, with strike UAVs executing precise attacks against targets that reconnaissance drones identify and track, while larger targets are held for a decisive artillery blow. This is a multi-element system that must be analyzed as a unified operational capability rather than as separate air threat and fires threat components.

The RSC's tactical significance is in its compression of the sensor-to-shooter timeline. Conventional targeting required multiple transmission steps, targeting authority decisions, and fire mission coordination that could take 20-45 minutes in a well-rehearsed staff. Ukrainian RSC cycles have been documented at under two minutes from drone visual acquisition to artillery impact. For IPB Step 3, this timeline compression changes the analytical requirement: the threat COA template must include the RSC activation sequence, the fires assets that the RSC feeds, and the combined sensor-fires coverage the integrated system creates. An S-2 product that correctly identifies where threat drones will fly but fails to connect that assessment to the fires that exploit the targeting data has produced half an IPB product for a whole threat system.

4.3 AI-Enabled Autonomy and the Post-Operator Threat

Ukraine conducted its first fully unmanned combat operation in December 2024, near Lyptsi north of Kharkiv, using ground robots and FPV drones in a coordinated attack on Russian positions without human pilots controlling the drones in flight. The MWI analysis documents that by 2025 Ukraine expected to field AI-enabled drone swarms with autonomous target recognition, and that both Ukraine and Russia are accelerating

AI integration into their UAS programs. The Russian defense sector has claimed neural network development for optical drone detectors with a reported 40 percent increase in detection range.

For IPB Step 3, AI-enabled autonomy changes the threat evaluation in three respects. First, the human network analysis driving left-of-launch intelligence becomes less decisive as operator dependency decreases: a drone that identifies and engages targets autonomously does not require an operator shift change that creates a maneuver window. Second, the threat COA template must address pre-positioned autonomous drones, which Defence Ukraine documents as sleeper FPVs modified with hibernator modules that can be placed in a forward position and enter low-power standby mode for days or weeks before remote activation. Third, EW responses that depend on disrupting the RF link between operator and drone become less effective against drones that navigate optically or inertially without GPS or RF command links.

5. Step 4 Revised: Determining Threat Courses of Action in the Drone Era

5.1 The Sensor Coverage Template: A New IPB Product

ATP 2-01.3 Step 4 produces threat event templates, situation templates, and a decision support template identifying named areas of interest and triggers for each threat COA. These products focus on threat force maneuver: where enemy ground forces will be at specific times, what terrain they will use, and what actions will indicate which COA they have adopted. For the UAS threat, these products are necessary but insufficient, because the operationally significant threat COA is not how enemy forces will maneuver but what the enemy's drone network will see, when, and how that intelligence feeds fires.

The required new product is the Sensor Coverage Template: a geospatial product mapping the assessed sensor coverage of threat UAS across the friendly area of operations under a given threat COA. The Sensor Coverage Template specifies for each identified or assessed threat UAS operating area: the EO and EO-IR detection ranges against each friendly signature category; areas of persistent coverage where drone ISR is likely continuous; areas of intermittent coverage depending on drone routing; detection probability for specific friendly activities including vehicle movement, command post emissions, logistics activity; and the correlation between observed drone activity in a given area and the fires effects that have historically followed.

This product enables the decision support template to address a new trigger category: not just triggers indicating which threat ground maneuver COA has been adopted, but triggers indicating whether a friendly element has been observed by threat UAS and is in the RSC targeting sequence. A reported drone observation of a friendly assembly area is not just a force protection report. Within the RSC's assessed sensor-to-shooter timeline, it is a predictive trigger: fires effects against that assembly area are likely within minutes. The S-2 providing that predictive analysis as a decision support product is the standard the current doctrinal framework does not specify.

5.2 Left-of-Launch Named Areas of Interest and High-Value Targets

The named areas of interest in the current Step 4 decision support template identify locations where specific activities indicate which threat COA is being executed. For UAS threat COA analysis, NAIs must be expanded to include drone-specific indicators providing left-of-launch warning: drone staging areas near forward positions, operator team assembly, relay aircraft launching to extend the control network, RF emission patterns consistent with ground control station activation, and logistics patterns associated with pre-strike drone preparation. These are the predictive intelligence triggers that enable C-UAS response before the drone is airborne rather than after it has completed its mission.

The high-value target list derived from Step 4 must also expand. ATP 3-01.81 identifies UAS as providing the threat with an aerial view enabling real-time intelligence and serving as a forward observer for fires. Disrupting that capability left of launch requires HVTs that are not the airborne drone but the ground network: operator teams and their assessed locations, ground control stations, charging and recovery infrastructure, relay aircraft launch positions, and fires integration nodes receiving UAS targeting data. These targets are harder to locate than airborne drones but their defeat eliminates the RSC reconnaissance function before it can generate a targeting solution.

5.3 COA Templates for Swarm Employment and Fiber-Optic Threats

The TSM 800 Red Air system at NTC can generate up to 150 simultaneous drones. Ukrainian and Russian forces have employed multi-drone swarm attacks in combat. The threat COA template must address swarm employment as a distinct COA with its own characteristics: simultaneous approach from multiple vectors to overwhelm single-track C-UAS systems; sequential saturation designed to exhaust kinetic interceptor magazines; and coordinated reconnaissance-strike sequences in which ISR drones identify and designate while strike drones attack. Each swarm characteristic requires a distinct analytical assessment and a distinct indicator set in the decision support template.

The fiber-optic drone represents a separate and analytically distinct COA. Because fiber-optic FPV drones have no RF signature, they cannot be detected by passive RF direction-finding systems that are a primary indicator in the current threat COA template. Their approach is detectable acoustically and visually but will not appear in the signals intelligence picture feeding the S-2's threat analysis. The COA template for fiber-optic drone employment must rely entirely on non-RF indicators: acoustic signatures, visual observation from air guards, optical detection triggers, and pattern analysis of previous fiber-optic employment identifying the operator's preferred approach corridors and target priorities.

6. The UAS-Integrated IPB Framework: Six Analytical Disciplines

The modifications to each IPB step described in sections 2 through 5 resolve into six analytical disciplines that must be institutionalized in FM 2-0 and ATP 2-01.3 revisions, in Military Intelligence School curricula, and in staff certification standards. Each discipline addresses a specific analytical gap that current doctrine leaves open.

Discipline 1: UAS Threat Network Analysis

Analogous to network analysis for IED threats, UAS Threat Network Analysis maps the human-machine network behind drone employment: operator teams, relay personnel, maintenance and charging crews, reconnaissance analysts, fires integration nodes, and supply chain. The product is a network diagram with assessed node locations, proficiency, shift schedules, and targeting priorities. S-2 sections must be trained to produce this product using pattern-of-life analysis, signal intelligence reporting, imagery, and human intelligence. The TRADOC G2 OE Enterprise Ukrainian UAS Tactics analysis published October 2024 provides the operationally validated threat model for building this analytical capability.

Discipline 2: UAS Sensor Coverage Modeling

UAS Sensor Coverage Modeling produces the geospatial assessment of what threat drones can see, at what ranges, under what conditions. The product requires knowledge of threat drone sensor payloads by group, their detection ranges against specific friendly signature categories including thermal, visual, acoustic, and RF, and the weather and terrain conditions that affect those ranges. This is a technical intelligence discipline requiring analysts with UAS-specific sensor knowledge. The product is the Sensor Coverage Template described in section 5.1, providing the commander with visibility into the threat's eyes rather than only the threat's position.

Discipline 3: Electromagnetic Terrain Analysis

Electromagnetic Terrain Analysis treats the RF spectrum as terrain, mapping areas where threat drone control signals are strong, degraded, or denied; where GPS is reliable or jammed; and where friendly EW can create denied zones shaping threat drone employment. This discipline requires coordination between the S-2 and the EW officer, producing the EM terrain overlay that informs both C-UAS response planning and maneuver route selection. Areas of GPS denial, where threat drones shift to fiber-optic or inertial navigation, require separate analytical treatment because standard EW responses become ineffective in those areas.

Discipline 4: Reconnaissance-Strike Complex Integration

RSC Integration analysis treats the UAS-fires combination as a unified threat system. The product maps the assessed locations of drone operators, the fires assets they feed, the sensor-to-shooter timeline for the assessed RSC configuration, and the geographic area in which the RSC can generate effects against friendly targets. This discipline requires the S-2 to integrate UAS threat analysis with fires threat analysis in a single combined arms threat template rather than treating them as separate analytical objects. The RSC-integrated COA template is the product that enables the decision support template to provide genuine predictive intelligence rather than post-event documentation.

Discipline 5: Left-of-Launch Indicator Development

Left-of-Launch Indicator Development identifies the observable activities that precede drone employment: operator team assembly, drone staging, relay aircraft launch, ground control station activation, RF emission changes, and logistics patterns associated with pre-strike drone preparation. These indicators populate the named areas of interest that the decision support template monitors. They are the predictive intelligence enabling C-UAS response before the drone is airborne rather than after it has completed its mission. This discipline requires deliberate indicator development work during the IPB process rather than reactive reporting during the operation.

Discipline 6: AI and Autonomous System Assessment

AI and Autonomous System Assessment evaluates the assessed autonomy level of threat UAS: whether drones require continuous operator control, operate within a pre-programmed waypoint framework, or employ AI-enabled target recognition allowing engagement without a human in the targeting loop. This discipline is increasingly critical as Ukraine's 2024-2025 AI integration demonstrates. The assessment drives the C-UAS response approach: AI-enabled drones operating independently of RF control require passive and kinetic defeat rather than EW-based disruption, and their employment patterns will not include the operator shift changes that left-of-launch intelligence depends upon.

Exhibit 2 | IPB Product Update Roadmap: Current Doctrine to UAS-Integrated Standard

IPB Step	Current Product	UAS-Era Extension Required	Lead and Timeline
Step 1: Define OE	Area of operations overlay; significant characteristics; initial collection plan	UAS OE Definition Product: drone operating radii; low-altitude airspace map; launch area assessment; EM spectrum overlay; signature detection ranges by friendly activity	MI Proponent (INSCOM/TRADOC G2); FM 2-0 and ATP 2-01.3 revision; 12-24 months
Step 2: Environmental Effects	Terrain analysis; weather effects; civil considerations overlay	UAS-Modified Environmental Effects: terrain channeling on drone range; weather by UAS group; EM terrain analysis; GPS-denied zone boundaries; vegetation and structure effects on optical detection	MI Proponent and EW proponent coordination; ATP 2-01.3 revision; 12-24 months
Step 3: Evaluate Threat	Order of battle; doctrinal template; threat indicator list; HVT list	UAS Threat Network Analysis; AI and autonomous capability assessment; RSC threat evaluation; fiber-optic and EW-resistant drone COA; left-of-launch HVT list covering operators, charging, relay, and GCS	TRADOC G2 OE Enterprise; MI school curriculum; ATP 2-01.3 and FM 2-0 revision; 12-24 months
Step 4: Threat COAs	Event template; situation template; decision support template; NAIs and TAIs	Sensor Coverage Template; RSC-integrated COA template; swarm COA template; fiber-optic COA with non-RF indicators; left-of-launch NAIs; RSC trigger set	MI Proponent and TRADOC; ATP 2-01.3 and ATP 2-01 revision; 12-24 months
Targeting Products	HVT list driven by platform and C2 node identification	Revise HVT list to include drone operator teams, GCS positions, relay aircraft, charging and recovery infrastructure, and RSC fires integration nodes	Fires and MI integration; FM 3-60 Army Targeting revision; 12-18 months
S-2 Training	MICCC and BOLC curriculum; IPB practicum with conventional threat	Add UAS Threat Network Analysis practicum; Sensor Coverage Template production; EM terrain analysis; RSC threat template; left-of-launch indicator recognition; NTC and JMRC drone environment exposure	MI School and TRADOC; BOLC and MICCC curriculum revision; 18-36 months

7. Conclusion: The Intelligence Failure That Precedes Every Other Failure

Every operational failure documented in the drone-saturated battlefields of Ukraine and the Middle East begins with an intelligence failure. A command post that moved into a position visible to threat UAS did not receive an intelligence product accurately characterizing the drone's sensor coverage of that terrain feature. A logistics convoy struck by RSC-coordinated fires minutes after drone observation did not receive an intelligence assessment predicting the RSC's sensor-to-shooter timeline and the fires assets it fed. A unit that exposed itself during a shift change that enemy drone operators had learned to exploit did not receive an intelligence assessment of the human network's schedule and the maneuver window that shift change created.

These are not failures of courage, leadership, or tactical skill. They are failures of the analytical framework that IPB is designed to prevent. The current ATP 2-01.3 framework was not designed for the UAS threat environment that now defines large-scale combat operations. The transparent battlefield, the reconnaissance-strike complex, the fiber-optic drone that cannot be found by RF direction-finding, and the AI-enabled system that does not require an operator shift change: none of these threat characteristics are systematically addressed in the analytical products that current IPB doctrine specifies.

The March 2026 Army doctrine overhaul, expanding FM 2-0 to address adversary UAS and revising FM 3-0 to incorporate drone operational imperatives, demonstrates institutional recognition of this gap. The revisions in progress are a necessary beginning. This paper argues that they require a specific and structured analytical extension: the six UAS-specific disciplines described in section 6 must be formally added to the IPB product set in the next ATP 2-01.3 revision and incorporated into the Military Intelligence School's core IPB curriculum. The intelligence officer is the staff proponent for IPB. In the era of UAS, that proponent role includes being the formation's expert on what the enemy's drones can see, when the operators rotate, how long it takes for a drone observation to become an artillery impact, and where in the terrain the formation can maneuver within the electromagnetic environment that shapes drone control. That expertise requires a doctrinal framework it does not yet fully have. Building it is the task that the drone dominance initiative implies and that the next ATP 2-01.3 revision must deliver.

Principal Sources

- ATP 2-01.3 Intelligence Preparation of the Battlefield (March 2019): four-step framework; S-2 staff proponency; information collection integration; threat evaluation methodology; dual-designated Army-Marine Corps manual
- FM 2-01.3/MCRP 2-3A Intelligence Preparation of the Battlefield/Battlespace (2009): foundational IPB doctrine preceding ATP 2-01.3; MDMP integration; COA development methodology
- FM 3-01.7 Appendix B: Air Intelligence Preparation of the Battlefield: aerial IPB framework; UAV launch site analysis; air avenue of approach methodology; ADA-aviation-S-2 integration requirements
- FM 2-0, Intelligence (under active revision, March 2026): expanding adversary UAS sections; individual Soldier drone-threat tasks; revision driven by drone dominance doctrine initiative
- FM 3-0 Operations (March 2025 revision): 'protect against constant observation' operational imperative; 'make contact with sensors, unmanned systems, or smallest element possible'; Russo-Ukrainian War vignettes integrated into doctrinal text

- ATP 3-01.81 Counter-Unmanned Aircraft System Operations (August 2023 and May 2025): UAS ISR, situational awareness, communications relay, weapon delivery, fires observer, and psychological warfare missions; commanders facing adversarial reconnaissance in operational environment
- CEPA: An Urgent Matter of Drones: Lessons for NATO from Ukraine (2025): transparent battlefield; British Army General 'no sanctuary' assessment; UAS military ecosystem requirements; kill chain compression in Ukrainian operations
- International Centre for Defence and Security (ICDS): Russia's War in Ukraine: Fortification for Drone Warfare (October 2025): kill zone deepened to 35-40 km; safe rear 10-15 km concept largely vanished; FPV and RSC density saturation point in 2023; drone-enforced attrition characterizing 2025 combat
- CSIS: Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience (May 2025): GPS jamming effectiveness; frequency agility adaptation; EW as defining characteristic; signals intelligence integration in drone operations
- CSIS: Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare (March 2025): RSC merging reconnaissance and strike UAVs with artillery in unified command system; first fully unmanned operation December 2024 near Lyptsi; approximately 2 million drones produced in 2024; 140 UAV complexes approved in first nine months of 2024
- Modern War Institute at West Point: Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine (January 2025): AI-enabled swarm development; Russian Rubicon Center; Ukraine's Unmanned Systems Forces established 2024; autonomous drone operations progression
- Small Wars Journal: The New Arms Race: Global Drone Dominance and America's Tactical Wake-Up Call (December 2025): left-of-launch intelligence; targeting pilot pipelines; Russian pilot shift change prediction enabling maneuver windows; three-month Moore's Law-like innovation cycle
- Defence Ukraine: FPV Drones in the Ukraine War: A Deep Dive (August 2025): fiber-optic FPV immune to jamming and RF direction-finding; sleeper FPV hibernator module; 300-400 km/h interceptor drones; Operation Spiderweb June 2025 strategic effects
- TRADOC G2 Operational Environment Enterprise: Ukrainian Unmanned Aerial System Tactics (October 2024): operator targeting patterns; shift change exploitation; distributed tactical innovation model
- Army.mil: Army Adapts Doctrine Force-Wide, Integrating Drone Lessons to Achieve Drone Dominance (March 30, 2026): FM 2-0 revision expanding adversary UAS sections; CADD two-tier doctrinal update structure; drone dominance as Army priority
- Inside Unmanned Systems: Army Rewrites Drone Doctrine Force-Wide as Drone Dominance Becomes Priority (April 2026): FM 2-0 intelligence update confirmed; FM 3-0 March 2025 revisions detailed; CADD-CoE doctrinal update mechanism described
- Military Review 2024: MG Joel B. Vowell and MAJ Anthony R. Padalino: existing mission command systems lack necessary technological capabilities; C-UAS systems require AI, machine learning, and automation to assist operator decision-making and enable simultaneous defeat mechanism employment
- Congressional Research Service R48477: Department of Defense Counter-UAS: Background and Issues for Congress (March 2025): UAS categorization by group; C-UAS doctrine requirements coordination; JCO training materials; FY2025 NDAA C-UAS provisions