DRONE DOMINANCE

Seizing War's New High Ground

JOHN ANTAL

Published in the United States of America and Great Britain in 2026 by
CASEMATE PUBLISHERS
1950 Lawrence Road, Havertown, PA 19083, USA
and
47 Church Street, Barnsley, S70 2AS, UK

Copyright © 2026 John Antal
John Antal has asserted his right to be identified as author of the work.

Paperback Edition: ISBN 978-1-63624-733-5
This book was typeset in India by DiTech Publishing Services.

Note: This PDF contains three extra appendices as additional online materials for *Drone Dominance*.

APPENDIX K

Provisional Drone Brigades

Leveraging the Army National Guard

Drone warfare is reshaping the battlespace at machine speed, and the U.S. Army has been slow to adapt. To reverse this trajectory, the Army can establish provisional drone brigades in the Army National Guard by adapting Army Reserve proposals, leveraging Transformation in Contact (TIC), and exploiting existing authorities and rapid-acquisition pathways to field unmanned systems at scale. No such formations currently exist—yet a pilot program provides the fastest, most practical path to test integration at scale and close this gap.

The Army National Guard is uniquely suited for this effort. Its dual state–federal mission spans homeland defense, disaster response, and combat deployments. It also brings a critical advantage: access to civilian technical expertise. By prioritizing experimentation with commercial off-the-shelf (COTS) drones, artificial intelligence (AI), and unmanned systems—drawing lessons from Ukraine and Israel—these brigades can close critical gaps in small unmanned aerial system (UAS) capability and deliver real-time sensing and strike to the tactical edge.

In war, these formations would augment the active force with trained, professional drone units. In peace, they would serve as a testbed for rapid innovation. The following phased approach provides a feasible path to execution.

Step 1: Authorization and resourcing

Secure authority and funding using existing mechanisms.

- Obtain congressional support through National Defense Authorization Act (NDAA) provisions or targeted legislation authorizing provisional units under Title 10 and Title 32 authorities
- Allocate funding from existing UAS and loitering-munition lines in FY2026 budgets
- Use rapid-acquisition pathways—including Other Transaction Authority agreements, Defense Innovation Unit programs, and commercial off-the-shelf procurement—to bypass traditional timelines
- Coordinate with the National Guard Bureau and state adjutants-general to align federal and state missions

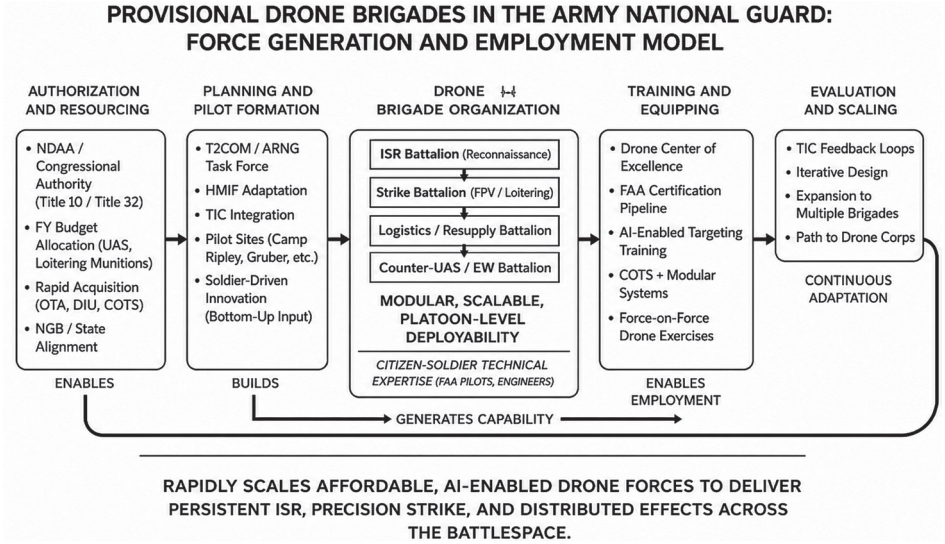


Figure K.1. Provisional drone brigades in the Army National Guard, a 12–18-month path to execution. This approach does not require new doctrine or force-structure approval cycles—it requires prioritization, integration, and disciplined execution. (Image by the author using ChatGPT)

Step 2: Planning and pilot formation

Design the force and select initial units.

Establish a joint task force under Transformation and Training Command and the Army National Guard Directorate
Adapt the Human–Machine Integrated Formation (HMIF) model
Select pilot brigades at existing Guard training sites (e.g., Camp Ripley, Fort Indiantown Gap, Camp Gruber, Camp Rapid)
Align with TIC expansion to ensure parity with active-duty modernization
Incorporate bottom-up input from soldiers to accelerate innovation and avoid institutional blind spots

Step 3: Structure and organization

Build modular formations designed for scale and employment.

Organize brigades into 3–5 battalions:
ISR (reconnaissance drones)
Strike (first-person view and loitering munitions)
Logistics and resupply
Counter-UAS and electromagnetic warfare (EW)Design for platoon-level deployability to support maneuver formations

Embed civilian technical expertise (Federal Aviation Administration [FAA] pilots, engineers, software developers)
Replace rigid training models with flexible, skills-based participation
Align equipment and doctrine with active force interoperability

Step 4: Training and equipping

Accelerate readiness through focused training and rapid fielding.

Establish a Drone Center of Excellence within the Guard
Integrate FAA certification into military training pipelines
Field affordable, modular COTS systems through DIU and Army marketplaces
Train AI-enabled targeting and real-time situational awareness
Conduct high-repetition, force-on-force "drone war" exercises

Step 5: Employment and scaling

Deploy, evaluate, and expand.

Federal missions (Title 10): augment divisions with ISR, strike, logistics, and EW support
State missions (Title 32): disaster response, border security, infrastructure protection
Use TIC feedback loops to refine tactics, organization, and equipment
Scale successful pilots into additional brigades
Inform future decisions on a dedicated Drone Corps

From proposal to risk

This concept provides a credible path to accelerate Drone Dominance. It leverages existing authorities, exploits Guard advantages, and aligns with ongoing transformation. But execution will determine success. The primary risks are not technical, they are institutional. If these risks are not addressed, the Army will field drone formations that exist, but do not matter.

Key risks to execution

1. Mischaracterizing drones as enablers rather than a warfighting system. If treated as expendable tools, the Army will fail to develop the expertise required to control sensing and strike. A designated proponent, career field, and doctrinal authority are essential.
2. Diffusion. The Army's instinct to distribute capability will dilute combat power. Drone Superiority requires mass, density, and persistence. These brigades must concentrate capability to generate decisive effects.
3. Failure to exploit National Guard talent. Civilian expertise is a strategic advantage. If constrained by rigid personnel systems, it will be lost.

4. Training stagnation. Drone warfare evolves rapidly. Training must emphasize repetition, adaptation, and combat realism, not compliance.
5. Acquisition delay. Traditional procurement cycles are incompatible with drone warfare. Systems must be fielded, adapted, and replaced at speed.
6. Survivability. Drone units must integrate sensing, strike, and protection. Without embedded EW and counter-UAS, they will not survive.
7. Fragile command and control. Units must operate under degraded conditions using distributed mission command.
8. Cultural resistance. Drone formations must be integrated into combined-arms operations or they will be sidelined.
9. Sustainment. Drone warfare is inherently attritional. Logistics must assume constant loss and rapid replacement.
10. Institutional friction. Title 10 and Title 32 authorities must be aligned in advance to enable rapid employment.

Getting this right and in time to make a difference

Provisional drone brigades in the Army National Guard offer a decisive step toward overcoming the Army's current inability to achieve Drone Dominance. They provide a practical, near-term mechanism to break institutional inertia and force adaptation at scale. By concentrating capability, talent, and experimentation in formations designed for the Land–Air Littoral, they move drones from the margins to the center of warfighting.

Within 12–18 months, the Army can stand up, test, and refine a true drone-warfare system, far faster than traditional force-development cycles. These brigades create a living laboratory that links sensing, strike, and protection into a unified kill web, generating the expertise required to achieve Drone Superiority in combat.

More importantly, they provide the mechanism to reshape how the entire Army fights. Without such a system, Drone Dominance will remain an aspiration. With it, the Army gains a credible path to transform concept into capability and regain the initiative in modern war.

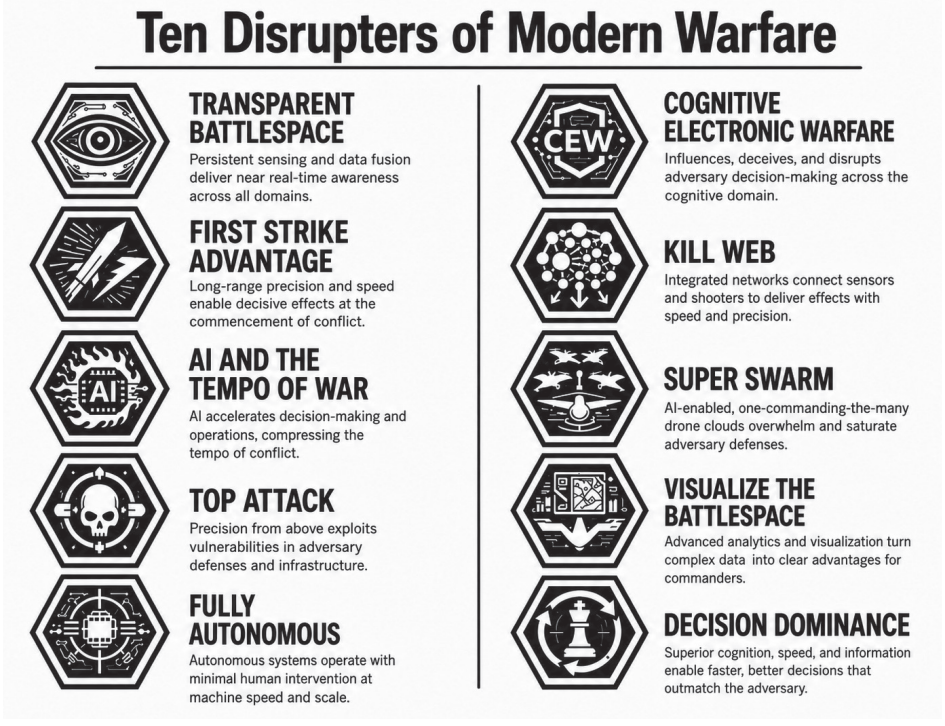
But this will not happen through process alone. It will require bold, inspired leadership willing to challenge institutional comfort and accelerate change. The Army has faced such moments before. Leaders like Brigadier General "Billy" Mitchell recognized that new technology demanded new ways of war, and acted despite resistance. The transition to Drone Dominance demands that same clarity of vision and willingness to act. Without it, the Army risks adapting too slowly to a battlefield that is already changing at machine speed.

APPENDIX L

The Ten Disrupters of Modern Warfare

This appendix provides a description of the ten disrupters of modern warfare as the conditions for establishing Drone Dominance and Drone Superiority. The ten disrupters of modern warfare define the emerging character of conflict in the era of intelligent machines.

A transparent battlespace, created by persistent intelligence, surveillance, and reconnaissance (ISR) from drones, space, and networked sensors, removes concealment and exposes movement, making it difficult for forces to mask or deceive and vulnerable to real-time targeting. This environment reinforces the first-strike advantage: the side that detects and strikes first gains decisive leverage as compressed timelines reward preemption and punish hesitation. Artificial intelligence (AI) further



accelerates this dynamic by driving the tempo of war to machine speed, compressing the OODA Loop (observe–orient–decide–act) and enabling continuous operations beyond human cognitive limits. At the tactical level, top-attack capabilities exploit the weakest surfaces of armored systems, while fully autonomous systems operate with minimal human input, scaling combat power at speed. In parallel, cognitive electromagnetic warfare adapts in real-time to jam, deceive, and disrupt enemy systems, making control of the spectrum decisive. These capabilities converge in the kill web, where networked sensors and shooters form a distributed, AI-enabled system in which any sensor can cue any shooter, replacing linear kill chains with parallel, resilient targeting. Super swarms—AI-enabled, one-commanding-the-many drone clouds—bring mass, redundancy, and precision to overwhelm defenses. Commanders now visualize the battlespace through advanced data fusion, gaining real-time situational awareness to fight in real-time, synchronize effects, and exercise mission command. The cumulative effect is decision dominance: victory goes to the force that consistently makes faster, better decisions under pressure. Together, these ten disrupters compress time, expand reach, and redefine combat power, forming the conditions for Drone Dominance and the pathway to Drone Superiority.[1]

APPENDIX M

Personal Mobile Devices in Training and Combat

Personal mobile devices are a beacon that can get soldiers killed

At Makiivka, Donetsk Oblast, Ukraine, on New Year's Day 2023, Russian forces concentrated personnel in a single facility while many soldiers used personal mobile phones. Those emissions created a dense electromagnetic signature that Ukrainian intelligence could detect, geolocate, and correlate with other intelligence, surveillance, and reconnaissance (ISR) sources. Once the location was fixed, Ukrainian forces rapidly passed the target into the fires system and executed a precision strike—widely assessed to be by HIMARS rockets—against the building. The combination of signal exposure, poor dispersion, and a fixed position turned the site into a high-payoff target. Russian officials later acknowledged that mobile-phone use contributed to the strike, while Ukrainian estimates placed the casualties in the hundreds. The incident demonstrates a core principle of the modern battlespace: unmanaged electromagnetic emissions can expose formations, enable rapid targeting, and lead to mass casualties within a compressed sensor-to-shooter cycle.[1]

After the attack, Russian officials attributed the losses at Makiivka to a lack of discipline among the soldiers themselves. Shifting blame to individuals, when leaders are responsible for enforcing standards, is a failure of command. Makiivka was a bloody lesson in discipline and leadership that American forces and their allies must take seriously.

U.S. Army policy on mobile devices in training and in combat

The U.S. Army does not have a single, universal prohibition on personal cell phones. Policy is mission driven and commander directed, enforced through operations security (OPSEC) and emission control (EMCON). The consistent principle is simple: uncontrolled personal devices are a targeting liability in a contested environment.

Training environment: in training, personal cell-phone use is restricted and controlled.

Basic Training/Initial Entry Training: personal phones are tightly limited or prohibited except during designated times.

Field Training/Combat Training Centers: personal devices are typically prohibited in the field. Observer–Controller/Trainers often enforce "no-phone" policies to replicate a contested electromagnetic environment. Use of personal devices can result in administrative action or removal from training.
OPSEC enforcement: units are trained to avoid geolocation, social-media exposure, and unauthorized transmissions.
Operational/Combat environment: in combat or high-threat environments, policy tightens significantly.
Commander's authority: commanders impose device restrictions, collection, or complete prohibition based on threat.
EMCON discipline: personal devices are treated as uncontrolled emitters that can be detected, geolocated, and targeted.
Operational risk: phones can reveal unit location, movement, and patterns.
Adversaries can exploit signals for targeting, cyber intrusion, or psychological operations.
Common practice in high-threat areas: devices are banned, collected, or secured before operations. Only approved, encrypted military systems are used for communication.

Doctrinal basis

Army guidance derives from established doctrine:

Field Manual 3-13, Information Operations, emphasizes OPSEC and protection of information and signatures.
Army Techniques Publication 3-13.3, Electronic Warfare Techniques, highlights the risk of electromagnetic emissions and enemy geolocation.
Army Regulation 530-1, Operations Security, directs protection of critical information, including electronic signatures.

Operational bottom line

Personal cell phones are not banned by default, but in any environment where the enemy can sense and strike, they are treated as a beacon that can get soldiers killed. Commanders therefore restrict or eliminate their use to preserve survivability, maintain discipline in the electromagnetic spectrum, and prevent the kind of targeting failures seen in Ukraine.

A persistent myth in U.S. military circles holds that if everyone carries a personal mobile device, the enemy cannot target the force because no distinct electromagnetic signature exists. This "stack of needles" argument is false in a modern, AI-enabled battlespace. Adversary ISR does not rely on single emitters; it exploits patterns, density, and correlation. Even in a saturated electromagnetic environment,

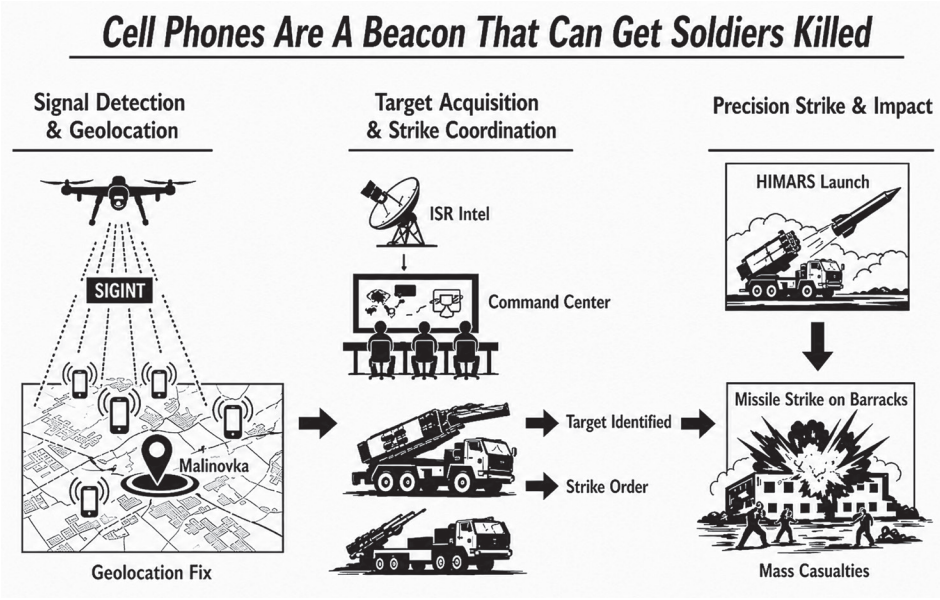


Figure M.1. Uncontrolled personal mobile devices emit detectable signals that can be geolocated, tracked, and targeted in near real-time. The Makiivka strike demonstrates how routine phone use can expose a concentrated force and enable rapid sensor-to-shooter fires with catastrophic results. Leaders must enforce strict emission control and prohibit personal communication devices in training and operational environments where the enemy can sense and strike. Discipline in the electromagnetic spectrum is not optional, it is a condition for survival. (Image by the author using ChatGPT)

machine analytics can cluster devices, detect anomalies in usage, and identify concentrations of signals that indicate command posts, assembly areas, or logistics nodes. Metadata—time, duration, colocation, and movement—reveals structure and intent without reading content. When multiple devices appear, move, and transmit together, they form a signature of a unit, not noise. Those signatures can be fused with other sensors—thermal, optical, and geospatial—to confirm targets and cue fires. In practice, more phones do not hide the force; they make it easier to find, fix, and strike. In a contested spectrum, uncontrolled emissions are not camouflage, they are beacons.

Policies on personal mobile devices vary by service, command, mission, and threat. When restrictions are imposed, the reasons are consistent: geolocation, wireless emissions, cameras, microphones, and stored data can expose locations, patterns, capabilities, and intent. During operations and high-end training, commanders may restrict, collect, disable, or prohibit personal devices to protect operations security, control emissions, and preserve force survivability.

Notes

Appendix L: The Ten Disrupters of Modern Warfare

1. John Antal, *Next War: Reimagining How We Fight* (Havertown, Pennsylvania: Casemate, 2023). Introduces the concept of the Ten Disrupters of Modern Warfare and their impact on the changing character of war. See also, "John Antal at the Maneuver Warfare Symposium," https://www.youtube.com/watch?v=mr9Wu3A5wbc; COL (R) John Antal, "The Changing Methods of Warfare," Fort Leavenworth, Kansas, October 23, 2023, https://www.youtube.com/watch?v=TcHnZxlHj0M&t=483s; James Eling, "132—Today's Lessons Learnt from Ukraine, Israel and Azerbaijan and the Ten Battlefield Disruptors for Tomorrow's Wars," with John Antal, *The Principles of War Podcast*, July 14, 2025, https://theprinciplesofwar.com/military-innovation/battlefield-disruptors/.

Appendix M: Personal Mobile Devices in Training and Combat

1. Tom Balmforth and Pavel Polityuk, "Russia Blames Mobile Phone Use for Deadly Ukrainian Strike in Makiivka," *Reuters*, January 4, 2023. Reports that Russian authorities attributed the Ukrainian HIMARS strike on a troop concentration in Makiivka to the widespread use of personal mobile phones, which enabled geolocation and targeting; Russia acknowledged 89 dead, while Ukrainian officials assessed casualties in the hundreds.