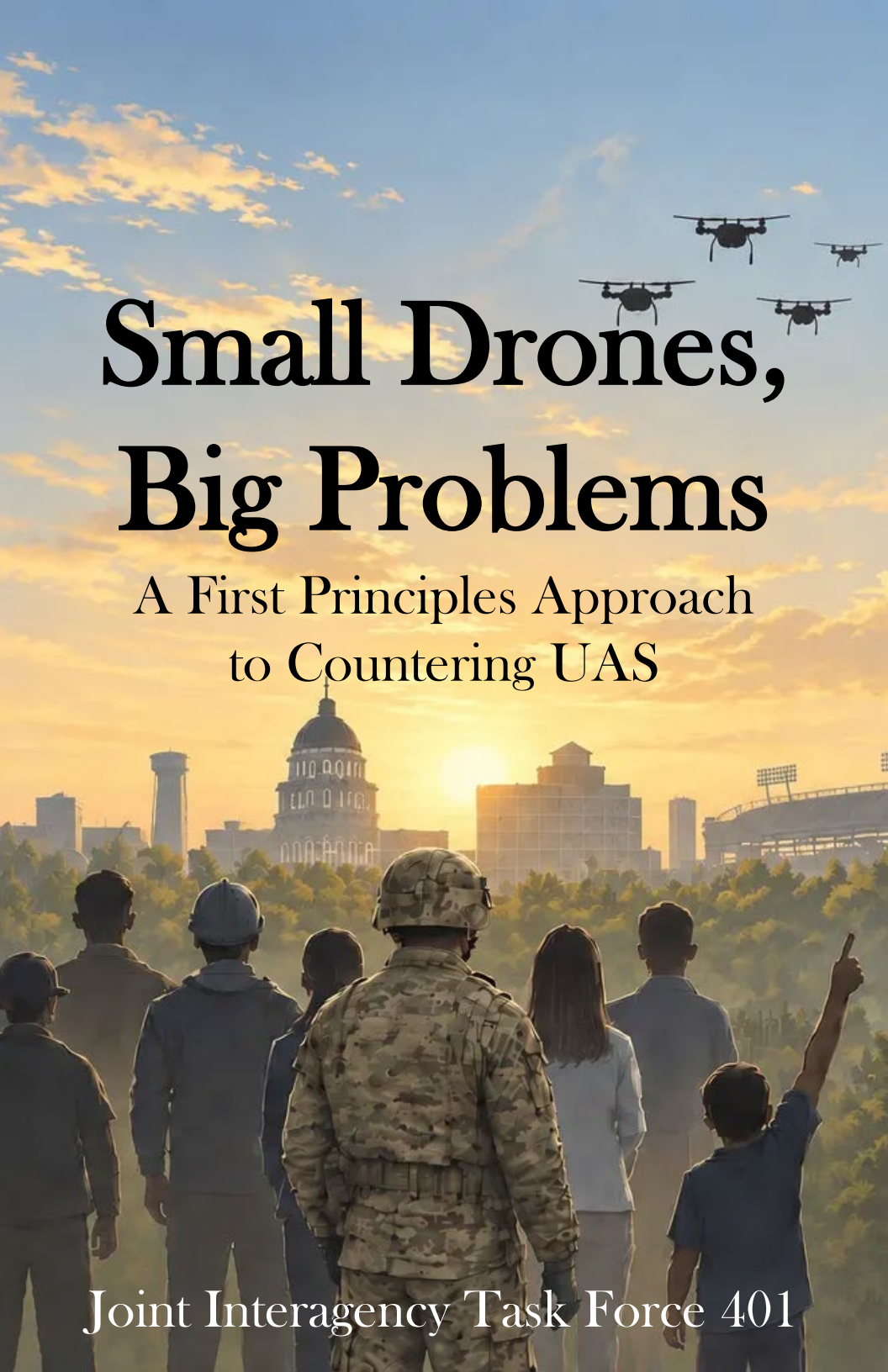


Small Drones, Big Problems

A First Principles Approach to Countering UAS

Joint Interagency Task Force 401

Foreword

Welcome to the world of countering unmanned aircraft systems (C-UAS). The proliferation of drones and adoption by both state and non-state actors is a national security concern that demands action. We must take prudent steps now and continue to evolve our defenses over time to protect our troops, bases, critical infrastructure, and the American people.

This guide is intended to provide a common foundation to shape our collective approach to this challenge. It is not a technical manual or detailed set of rules, like doctrine. Rather, this guide outlines first principles to orient ourselves to meet the new drone threat. It is meant to be read from start to finish and draws on combat experiences and examples from the U.S. homeland to inform drone protection principles.

These principles are important to prevent a drone attack before it occurs or defend against one that is underway. They are also not unique to the U.S. military. Drone protection principles apply equally to federal agencies and departments as well as state and local law enforcement across our nation.

This guide is organized into three main sections. First, it explains what drones are and how adversaries might use them. Second, it outlines what it means to protect against drones and how we prepare to do so effectively. Finally, it examines important factors that enable successful counter-drone operations, including the electromagnetic spectrum, the network that controls counter-drone sensors and effectors, and artificial intelligence.

While there is no silver bullet to protect against drones, the threat can be mitigated if we are proactive, work with partners across the government, and build a layered defense. It is imperative to give our warfighters the tools, technologies, and training they need as rapidly as possible to defend the homeland. We have faced novel challenges before, and we should not be intimidated by this one. On the contrary, we should lean in and take every possible step to remain ahead of our adversaries. Together, I'm confident that we will.



MATTHEW ROSS
BRIGADIER GENERAL, UNITED STATES ARMY
DIRECTOR, JIATF 401

This publication is available at the
U.S. Department of War's Drone Dominance Spotlight site
(https://www.war.gov/Spotlights/Drone-Dominance/)

Notes

Intentionally Left Blank

Department of War
Joint Interagency Task Force (JIATF) 401
4800 Mark Center Drive, Suite 10E12
Alexandria, VA, 18 June 2026

SMALL DRONES, BIG PROBLEMS:

A First Principles Approach to Countering-UAS

INTRODUCTION

THE "HAPPY TIME" **2**
Why This Book—Why Now? 3
Establishing "First Principles" 4

PART I: DRONE WARFARE

CHAPTER ONE **8**
Is It a Bird, Plane, or Drone? **8**
From Science Fiction to Chinese DJIs: The Genesis of Drones 9
The Cocktail Party Definition of a Drone 13
Looking Through the Enemy's Eyes 16

CHAPTER TWO **17**
The Four Ps of Drone Threats **17**
The Four Ps of Drone Threats 20
How Drones Will Be Used 23
A Complete Drone System 24

PART II: PROTECTING AGAINST DRONES

CHAPTER THREE **27**
The Five Ds of Protecting Against Drones **27**
The Five Ds of Drone Protection 29
How Can I See Trouble Coming as Early as Possible? 29

How Do I Mess Up Their Plans If They Attack Anyway? 32
How Do I Make an Attacker Turn Back Because Things Are Too Risky or Difficult? 34
What Is My Last Resort to Stop the Threat? 35
How Do I Make Good Decisions Under Uncertainty? 37
The Network as a Tool 39

CHAPTER FOUR 42
The Five Ds In Practice 42
Protecting Against Drones is an Outcome, Not a Moment 43
Buy Time (Get "Left of Launch") 44
Teamwork Makes the Dream Work 45
Practice Makes Perfect 46
It All Comes Down to Discipline 49
What Success Looks Like 49

PART III: KEY CONSIDERATIONS

CHAPTER FIVE 54
Protecting Against Drones In New Terrain 54
I Don't Understand—This Was Working Before 55
How Can the Physical Environment Affect Drone Protection? 56
How Can the Electromagnetic Spectrum Affect Drone Protection? 58
The Basics of Jamming 59
When Environments Collide 60

CHAPTER SIX 64
What Is The Role of Artificial Intelligence? 64
Artificial Intelligence Helps 65
Clearing the Air 66
Artificial Intelligence, Real Protection 69
This Time, With Artificial Intelligence 71

CONCLUSION **72**
Ending the "Happy Time" **72**

APPENDIX A **78**
A Professional Glossary **78**

APPENDIX B **86**
An Annotated Bibliography for Joint Doctrine **86**

Intentionally Left Blank

Introduction

The "Happy Time"

Introduction

The "Happy Time"

It was 1939, in the North Atlantic Ocean, and a night watchman stood on the bridge wings of the *HMS Resolute*. He was scanning the dark waters with a mix of boredom and dread.

He stamped his boots and muttered to himself, "Nothing moves out there." But who knew what really lurked out there under the water.

On the horizon, the sailor thought he saw a hard, curved line against the choppy line of the sea. A feather of seafoam appeared in the middle. He stopped in his tracks.

What was that, the back of a submarine? A periscope?

The Germans called the start of U-boat operations the "happy time"—before the Allies (consisting of China, Russia, the United Kingdom, and the United States) knew how to react and how to protect themselves.

But the "happy time" didn't last forever. British and American ships learned to adapt to the threat by implementing a convoy system to protect shipping lines, using escort ships, and developing new technologies like sonar, radar, and depth charges.

As the war progressed, German U-boats continued to threaten Allied maritime shipping and operations. But U-boats did not end the war, leading to Germany's victory.



WHY THIS BOOK—WHY NOW?

Drones have enjoyed their "happy time" as well. They are versatile, agile, and adaptable tools. Like German U-boats, however, drones don't win wars. Iran's use of drones, specifically the Shahed-136, to target U.S. military forces and interests across the Middle East following the start of Operation Epic Fury on February 28, 2026, is one clear example. While Shahed-136 drone strikes accounted for 66% of Iran's counterattack operations during the initial phase of Operation Epic Fury from February 28 to March 9, 2026, they did not erode the U.S. military's combat power or undermine America's resolve.

From small outposts across the Middle East to trench lines in Ukraine, drones have changed how Soldiers experience war. They erase safe areas, give enemies a constant view of the battlefield, and instill fear. Drones are not going anywhere; they are here to stay, and all of us must be trained and ready to deal with them, both at home and abroad.

Yet the story about drones is not one of a "silver-bullet" in war. It is about a cat-and-mouse game between adversaries. Initially, drones exploit defenses that are mismatched to their use. Radar systems may be built to spot large planes or fast missiles, not small drones flying low and slow.

Learning militaries adapt and innovate, repurposing existing defenses and building new ones to address vulnerabilities exploited by drones. They change how they think about drones and how they fight.

A good example is the U.S. military's response to Iran's use of Shahed-136 drones. In response, the Department of War delivered the most effective counter-drone capabilities to Soldiers deployed across U.S. Central Command in the Middle East. Some of these capabilities were quickly transferred from Ukraine and training was provided by Ukrainian drone experts, helping to enhance protection against Iran's use of drones to attack U.S. military bases and critical infrastructure across the region. In part, these efforts helped drastically reduce the frequency and effectiveness of Iranian drone attacks.

ESTABLISHING "FIRST PRINCIPLES"

This book is an introduction to drones and drone protection. It is for everyone—from frontline Soldiers to federal agents to local law enforcement. The fundamentals of drone employment and drone protection can be learned. Once you know the fundamentals, you can start adapting and innovating to counter the threat of drones.

The first step to planning is understanding the problem and ensuring that everyone on your team understands the problem in the same way.

Too often, when people talk about drone warfare, they jump to extremes. They imagine complex and terrifying drone threats. They feel like they need expensive, fancy solutions to protect against drones.

The truth about protecting against drones is a lot less glamorous. In most cases, you can effectively protect yourself against drones by evaluating the threat methodically and approaching it pragmatically. Often, the best defense is a good offense. Targeting drone operators, as well as the component parts of drones, can remove the threat before it materializes.

Given this reality, this book establishes "first principles" for protecting against drones. It is guided by two key questions. First, what things do you need to understand about drones and drone protection to tackle the problem? Second,

what are those fundamentals that make protecting against drones go from seemingly impossible to eminently doable?

So, what is a drone anyway? How does the enemy use drones? We address these questions across two chapters in Part I—Drone Warfare—before introducing principles to protect against drones.

Intentionally Left Blank

Part I: Drone Warfare

Is It a Bird, Plane, or Drone?
The Four Ps of Drone Threats

Chapter One

Is It a Bird, Plane, or Drone?

Mud was a constant companion—a cold, wet reminder of the grim reality of the front lines near Bakhmut, Ukraine.

The pungent smell of gunpowder was thick in the air.

A Ukrainian infantryman, huddled in the relative safety of his trench, flipped open a case on the ground and pinched the thing inside with two gloved fingers.

It looked like something meant for a Batman action figure—a tiny, black helicopter-looking thing, about the length of his right hand.



The Ukrainian Soldier placed it on his palm and used his other hand to pull out the covered tablet, balancing it carefully on his knees. A few taps on the tablet screen and the tiny rotor blades on the helicopter began to whirl. The Soldier's eyes scrolled over the battery icon to check that it was charged and then, glancing up at the gray sky, he gently threw the machine into the air.

The little helicopter stabilized mid-air, like a hummingbird lifting off a feeder, and then zoomed away.

The Soldier's eyes were now on his video feed that showed a desolate landscape peppered with shattered trees and smoldering houses. He found a ruined wall on the landscape and began to steer the drone along it.

After some time, a farmhouse came into view and the Soldier steered the machine so it could clear a roof. He switched to thermal imagery on his tablet and two heat signatures appeared on the screen, huddled close for warmth inside the house below. After taking several snapshots and a short video, the Soldier turned the little helicopter homeward.

While the word "drone" inspires mental images of a spiderlike machine careening above a park or sporting event, not all drones look alike. Some, like the nano drone flown by the Ukrainian Soldier, are as small as a songbird and can fit in your hands. Others are larger than the biggest prehistoric pterosaurs and weigh as much as a juvenile humpback whale.

The pages ahead will tell you enough about drones to be "dangerous." They give a simple definition of a drone, explain its key components, and provide a simple survey of drone types. While drones may appear to have emerged out of nowhere, they are part of a longer evolution story of militaries' interests to see further, extend their operational reach while protecting their own forces, and exploit opponents' vulnerabilities.

FROM SCIENCE FICTION TO CHINESE DJIs: THE GENESIS OF DRONES

Drones are not an overnight phenomenon.

In his 1965 best-selling book, *Dune*, Frank Herbert concocted the "hunter-seeker" drone—a small, remotely controlled tadpole-like flying robot used to assassinate unsuspecting targets. But while this science fiction idea

felt newish in the 1960s, it was an adaptation of a concept that was not so new, even in 1965.

For as long as humans have fought wars, they have looked for ways to see and strike their enemies from a greater distance. The farther you are from your enemy, the safer you can stay and the more time you have to react. We've come a long way from close combat with broadswords and battle axes.

Over time, the quest for greater operational reach or standoff included the employment of humanless machines to do the work of humans—the work of seeing, maneuvering, and shooting. The examples go back a long way.

In 1849, Austria tried to bomb Venice using pilotless balloons filled with explosives. The wind carried them toward the city. During the American Civil War from 1861-1865, both the Confederate and Union sides used balloons to watch enemy movements from above.



These early systems were hard to control and easy to defeat but foreshadowed the promise of seeing and striking with crewless craft. In 1936, a

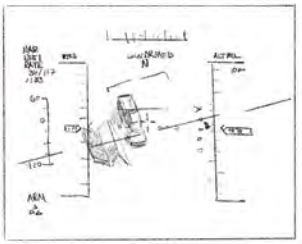
French writer named Georges Bernanos imagined that "tomorrow, the best killers will kill without risk. At thirty thousand feet above the ground, any bloody engineer, nice and warm in his slippers, surrounded by specialist workers, will only have to flip a switch to assassinate a city and then head quickly for home, his only fear being that he will miss his dinner."

As technology improved, militaries continued to build better and better vessels. By the great wars, the Allies were experimenting with more sophisticated pilotless aircraft. These included the wooden biplane "Kettering Bug" in World War I and the radio-controlled "Queen Bee" in World War II, a name that many believe inspired the word drone.

In the Cold War era that followed, the United States tested and flew unmanned "Lightning Bug" drones during thousands of reconnaissance missions in Vietnam. Through the end of the 20th century and start of the 21st century, drones continued to proliferate. Following the terrorist attacks of September 11, 2001, during the "Global War on Terror," the U.S. military deployed drones for both reconnaissance and attack.

Other countries, such as Iran, observed the U.S. military's successes with drones during conflicts in Afghanistan, Iraq, and Syria, and adopted these capabilities with the intent to enhance their combat power. Drones became ubiquitous, and drone technology rapidly accelerated, following Russia's invasion of Ukraine in 2022. One major change was the use of First Person View, or FPV, drones. These drones sent live video feeds to pilots wearing headsets, making it feel as if they were inside the aircraft. FPV drones were widely used in Ukraine, where they flew fast and low toward their targets. By some accounts, though only 20-40% of Ukrainian drones found their targets, they accounted for 60-70% of damaged or destroyed Russian systems, and 70-80% of Russian casualties.





Jamming devices also became more sophisticated during the war in Ukraine, causing both Russia and Ukraine to experiment with more survivable drones. Drones increasingly used fiber optic cables to fly; these fiber optic cables were literally connected to the ground. Drones also rapidly switched radio frequencies that allowed operators to remotely control them. Still other drones relied on artificial intelligence (AI) during their final moments of flight. If their radio signals were jammed, they could still find and strike targets.

Drones also spread beyond the air. Unmanned ground vehicles and unmanned boats became a part of modern war. In 2022, Ukraine used an unmanned surface vehicle to help sink Russia's flagship cruiser in the Black Sea. China also experimented with unmanned, robotic "dogs" that were mounted with high-caliber machine guns. Developments like these show how unmanned systems can change warfighting on land, sea, and in the air.

Drones are not only tools of militaries, however. Some of the most dangerous uses of drones come from groups with little money and training. The Islamic State in Iraq and Syria used cheap and commercially available drones, which it outfitted with cameras and grenades, to watch and strike U.S and coalition troops. Hamas used small drones during its surprise attack on Israel in October 2023. The Houthis in Yemen used small drones to strike ships in the Red Sea. Mexican drug cartels used small drones to attack each other along the U.S. southern border.

Besides launching salvos of Shahed-136 drones against the U.S. military during Operation Epic Fury, Iran also explored the possibility of conducting a drone attack in the U.S. homeland. Intelligence indicated that an Iranian sleeper cell aspired to conduct a surprise drone attack somewhere in California, perhaps against a religious site, as retribution for Operation Epic Fury.

Each of these examples represent just one more step in drones' ongoing evolution. With each new era, drones have become more capable, flying farther, staying aloft longer, and carrying more—all without risking pilots' lives. From balloons drifting over 19th century battlefields to the AI-enabled systems today, drones reflect how militaries adapt old concepts into ever more sophisticated fighting tools.

In sum, drones are not a magic weapon. They have resulted from incremental improvements on older ideas to see further, extend operational reach while reducing battlefield risks, and exploit adversaries' vulnerabilities.

THE COCKTAIL PARTY DEFINITION OF A DRONE

With all these examples, the definition of a drone can seem confusing.

As a starting point, drones are systems that operate without a person physically onboard the platform. They may be small or large, remotely-controlled or automated, tethered or free. They can operate in the air, on the ground, under or on water, and in space. Despite these differences, all drones share a common feature. They don't have a pilot onboard; they are uninhabited.

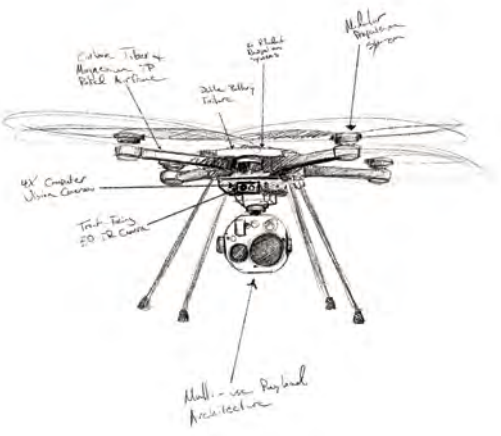
Is a balloon a drone? Is a paper airplane a drone?

No. Drones move with a purpose and have similar hardware and software components, including a propulsion system, power source, controller, communications, and enabling software.

Drone hardware includes core components that enable flight and operation.

The drone holds all parts together. The propulsion system—often using efficient brushless DC motors—provides movement, and a lithium polymer battery supplies power, while the controller processes data and directs motion using input from sensors such as an inertial measurement unit, Global Positioning System, barometer, and compass. Communication hardware links the drone to an operator, and the payload consists of whatever the drone carries, from cameras to mapping tools to munitions.

Drone software consists of layered programs that control stability, coordination, navigation, and human interaction. Firmware handles critical low-level tasks such as stabilization, speed, and data processing while the operating system or middleware ensures the drone's sensing, thinking, and movement functions work together. Navigation and control algorithms manage flight planning, obstacle avoidance, and complex maneuvers like autonomous landing, and control station software allows operators to plan missions, monitor status, view video, and manually guide the drone.



Many of these components can be enabled by AI. For instance, the drone's sensors can see and identify objects for the operator, the control system can decide how to execute a mission without direct commands from the pilot, or the drone can adjust its path of travel in real time to intelligently avoid

obstacles or collisions. In Chapter Six, we will discuss more about the implications of AI for drone warfare.

Drones also may also be remotely-controlled or automated. All drones are systems. Drones include operators, computers that process video and sensor data, networks that carry signals, and crews who employ, recover, and maintain them. If any one part of this system fails, the drone becomes ineffective.

People often classify drones by size rather than by components or individual systems, thinking of them in terms of small, medium, and large drones. This simple rubric is helpful to understand how and why militaries use drones.

Small drones, such as commercially available Chinese DJI models, typically fly at very low altitudes, often between 100 and 500 feet above the ground. Their speeds usually range from 20 to 45 miles per hour, and their effective range is limited, often one to ten miles from the operator. Most small drones can stay airborne for 15 to 40 minutes. Because they are lightweight, quiet, and easy to launch by hand, they are well suited for short-range surveillance, spotting targets, adjusting fires, or dropping small explosives onto personnel or vehicles.

Medium drones, such as the Turkish TB2 and Iranian Shahed-136, operate at higher altitudes, commonly between 15,000 and 25,000 feet. They fly faster, usually around 70 to 140 miles per hour, and can travel 150 to 300 miles from their launch point using satellite or relay communications. These drones can remain airborne for 20 hours or more and often carry guided weapons. Medium drones strike a balance between cost and capability, making them effective for reconnaissance, precision attacks, and supporting ground forces.

Large drones, such as the MQ-9 Reaper, fly the highest, fastest, and farthest of all. They operate at altitudes up to 50,000 feet, cruise at speeds around 200 to 300 miles per hour, and have ranges exceeding 1,000 miles. Some can stay in the air for 24 to 30 hours. Militaries prize these drones because they provide continuous overwatch, carry multiple sensors and weapons,

and can observe, track, and strike targets across regions while remaining largely reusable. But they are vulnerable to air defenses and expensive, which prohibits their adoption by many countries and especially non-state actors, like terrorists.



LOOKING THROUGH THE ENEMY'S EYES

To fully understand the drone threat, it's not enough to know what drones are and how they've evolved over time. We must understand how people use drones to do harm—how they scout, intimidate, attack, and exploit their opponents' vulnerabilities.

We discuss this question in the following chapter. We examine the tactics and techniques adversaries use to turn even simple, small drones into weapons of war. From this understanding, we can better prepare to protect against drones at home and abroad.



Chapter Two

The Four Ps of Drone Threats

The sun had just risen over the airfield. A light frost clung to the chain-link fences, as a military policeman, or MP, patrolled the perimeter, driving along his usual route. The morning was quiet, normal, and routine. He paused to look up and down the fence line and observed nothing unusual.

That was the whole point.

A few miles away, a flatbed truck carrying containers parked on the shoulder of a service road that rarely saw traffic. Dusty and dingy, it was the kind of truck people stopped noticing years ago.

The driver was reviewing his delivery paperwork, trying to figure out why the delivery location was there. He reached for his phone to call the dispatch operator as he threw on his hazard lights. To anyone passing by, it looked like a vehicle waiting for a tow. Inside the wooden cargo box on the truck bed, tucked beneath a false roof, dozens of small drones sat in neat rows, silent and patient.

The driver—standing outside—leaned against the door of the cab, smoking a cigarette. He exhaled before he felt the truck shudder. He jumped away from the cab as he saw the false roof of the wooden cargo box blow open. A whine rose from the box behind him like a swarm of bees.

The first drone slipped out of the wooden cargo box, rising into the air. Then another. And another. Within seconds, the sky was filled with tiny shapes, blowing downwash and grit onto the astonished driver. They climbed steadily, moving loosely in formation. Minutes later they were specks, drifting quietly toward the base.

Back at the airbase, an MP paused for a second before driving on. He thought he heard something through his open window. It may have been a distant hum or nothing at all. He scanned the horizon, and up and down the fence line. Though he strained his eyes, he only saw the pale light of the morning sky. Shrugging off his paranoia, he continued his patrol.

As he approached the airfield, the MP finally heard it clearly—a faint metallic buzz, like a dental drill. Frowning, he squinted upward, again. For a moment he couldn't make sense of what he was seeing. The shapes were too small, too fast, and too numerous. His radio crackled to life, filled with confused voices, overlapping questions, and someone shouting for confirmation.

The drones descended in a coordinated wave, each one following a preprogrammed path. They weren't hesitating or reacting, they were executing a task.

Inside the main command post and air traffic control station, alarms began to blare. Personnel scrambled to screens, trying to understand what was happening and how something so small had appeared so suddenly. Someone yelled for action.

By then, the drones were weaving through the outer perimeter of the airbase, slipping past defenses designed to stop people, vehicles, or planes. The MP froze for a moment, caught between instinct and disbelief. Then his training kicked in—he ran for cover as the drones started dropping explosives on the airfield, striking facilities and aircraft parked in the open.

The whole attack lasted mere minutes. When it was over, the base was still standing, but smoke and shock hung in the air. People slowly emerged from bunkers, dazed and confused, and started to piece together what had happened.



This vignette is not science fiction. It is based on Ukraine's "Operation Spider's Web." On June 1, 2025, Ukraine deployed over 100 drones to strike Russian military bases and destroy one-third of the country's strategic bombers. Ukraine used unsuspecting deliverymen to get the drones to their target.

For us, this story is important for two reasons. First, it shows the versatility of drones. You don't need high-end craft to cause chaos and destruction. Small, cheap, commercially available, and easily weaponized drones—deployed creatively—can overwhelm defenses and defenders.

Second, the story also demonstrates the complexity of Operation Spider's Web. It resulted from over two years of intelligence gathering, planning, and coordination. Most drone attacks are not like Operation Spider's Web. Rather, they are often ad hoc and opportunistic, seeking to exploit weaknesses in an opponent's defenses, such as an airbase that is not hardened against drones.

So, how do you plan and prepare for the drone threat? What is possible? What is likely?

THE FOUR Ps OF DRONE THREATS

While drones seem to be everywhere, not every drone is the same and not every drone is a threat.

As discussed in Chapter One, drones come in a variety of types, sizes, and have different payloads. They can be controlled in many ways, using different types of communication. They can also be used for different purposes—to kill, watch, and aid. Finally, drones are used by millions of people globally, with different intentions, ranging from recreational hobbies to violence.

To accurately assess the drone threat, and begin thinking of a drone protection plan, it's helpful to think through four factors—the person (operator), platform (drone), process (control), and payload (purpose).

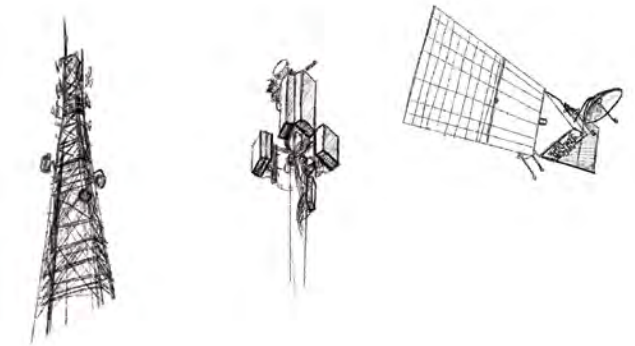
First, a drone by itself is just a piece of equipment. Paired with an operator it can become a toy, a tool, or a weapon. If you think you face a drone threat, you should first ask: *from whom*? Who are the drone operators in range of your area of operations? For instance, consider the characters that could pose a drone threat to your personal home. Is there a peeping Tom, a nosy neighbor, a porch pirate, or a cat burglar? What about more nefarious actors, like car thieves or home invaders?

Second, should you determine a drone threat may exist, you should then ask: *what kind of drones are you likely to encounter*? Consider what drones and drone materials are prevalent in your area of operations. DJI quadcopters? Fixed-winged drones? 3D printed drones? Fiber optic drones?

These platforms have different strengths and weaknesses, which provide important clues about their range, altitude, and intentions. Small, fixed-wing drones are unlikely to drop munitions because they cannot stabilize, but they generally have longer endurance than a quadcopter of similar size. Conversely, quadcopters can sit and surveil a specific location with more accuracy because they can hover in place.

When confronted with what you believe is a drone threat, you should then ask: *what processes of drone control am I likely to encounter*? The answer will provide critical clues that further help you to shape a drone protection plan. These include how the drones you encounter will look, sound, and act; how they will takeoff, land, and behave in flight; how the operators will launch and pilot them; and how many personnel are required to maintain and recover drones.

The most common form of drone command and control today is through radio frequency. Most commercial drones—used for either benign or malign purposes—are remotely-controlled using radio frequency (RF). Many drones are also able to fly-by-waypoint, meaning their flight path is managed by pre-programmed Global Positioning Systems waypoints. Some drones can receive adjustments in flight, while others must return to their launch point for a new flight plan. Other drones, as discussed before, can be controlled via tether or cable.



As you might suspect, drone command and control is evolving at a rapid rate, as new hardware and software become more capable and autonomous. Drone manufacturers are building add-ons that allow drones to fly over mobile data via cellular towers. This gives operators the same flexibility as drones controlled remotely through RF. It provides greater drone flight ranges, assuming the signal remains strong. With artificial intelligence (AI), drones are now able to incorporate image recognition into their targeting and navigation.

Finally, you should ask: *what is the purpose of the drone*? Thinking through potential purposes will help you anticipate the drone threat and predict behaviors. For instance, are drones likely to fly low and slow, hugging the terrain? Or are they likely to pop-up and hover over the terrain from a safe distance?

A drone's purpose is defined by the combination of its payload and the operator's intent. Drones can carry munitions ranging from small grenades to precision-guided weapons, cameras, and surveillance or electronic sensing equipment capable of detecting or jamming communications and radar, and supply bundles such as medical aid or fuel. Sometimes drones themselves, such as loitering munitions or one-way attack drones, also called "kamikaze drones," are the munition. How these capabilities are used depends on what the operator seeks to achieve—whether to see, hear, distract, disrupt, embarrass, intimidate, hurt, or kill.

A drone can achieve its purpose even if it is defeated. Responding to drones drains resources, triggers unnecessary activity, or diverts attention. If the operator's goal is to disrupt an event, forcing airspace or road closures could be a "success," even if the drone crashes. If the goal is reconnaissance, a few minutes of recorded video may be enough. Once gathered, the drone does not need to survive. When the goal is smuggling, it may be sufficient to reach a release point and not return home.



HOW DRONES WILL BE USED

Drones are used in many ways but, like everything, operators draw from common tactics. These range from employment of first-person view attacks, a signature of the Ukraine War, to hunting for armored vehicles, ambushing convoys, and intercepting helicopters and jets.

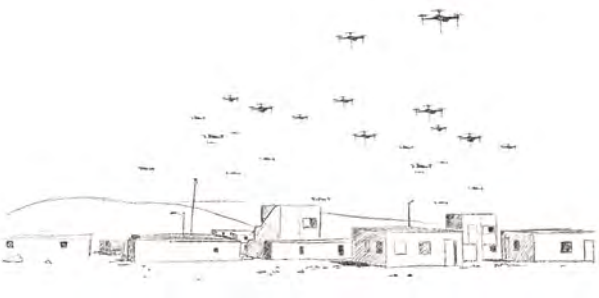
Small quadcopter drones like the Chinese DJI Mavic are frequently used for reconnaissance, artillery spotting, and dropping small munitions, while larger multi-copters drones carry heavier payloads or act as communication relays. Longrange, oneway attack drones like the Iranian Shahed-136 are used for deep strikes on cities, infrastructure, and logistics hubs, are often used in waves, and can integrate with missiles to overwhelm air defenses, airfields, energy facilities, and industrial sites far from the front. Iran used these tactics, and struck these targets, following the start of Operation Epic Fury with the intent to influence global markets and undermine the United States' resolve.

Drones are also increasingly deployed in teams, or swarms.

There's much debate about what makes a swarm. Swarms fall into two broad categories, mass and intelligent. A mass swarm refers to groups of unmanned aircraft, launched together or in close sequence, to affect a common objective, with notable examples being Ukraine's Operation Spider's Web and Iran's use of drones during Operation Epic Fury.

An intelligent swarm happens when multiple autonomous drones operate collaboratively to achieve a common objective. Using AI-enabled onboard processing and communication, intelligent swarms adapt, reposition, or divide tasks without constant human control. These swarms can include drones carrying different payloads, letting them map terrain, confuse defenses, or gather intelligence simultaneously and from several angles. Their strength comes from numbers, cooperation, and the ability to overwhelm defenses through sheer quantity and complexity.

There will be more about AI and its utility in drone warfare in Chapter Six.



A COMPLETE DRONE SYSTEM

You may be familiar with the mantra, "guns don't kill people; people kill people."

The same logic can be applied to drones—more resoundingly even. People generally use guns for sport, hunting, and violence, but they use drones for everything from wedding photos to missile strikes.

When considering the threat of drones to you or your unit, consider the four interacting parts of drones—the person, platform, process, and payload. The clues you will discover in considering these factors will help you understand whether a drone threat exists and what you can do about it.

Once you have a complete picture of the drone threat, you can shift from targeting or mitigating drones in isolation, to disrupting the whole threat—by streamlining your decision-making processes, diversifying your countermeasures, and investing in tools that address operators and supply chains. This approach is driven by key drone protection principles that we introduce in the next two chapters.

Intentionally Left Blank

Part II: Protecting Against Drones

The Five Ds of Protecting Against Drones
The Five Ds in Practice

Chapter Three

The Five Ds of Protecting Against Drones

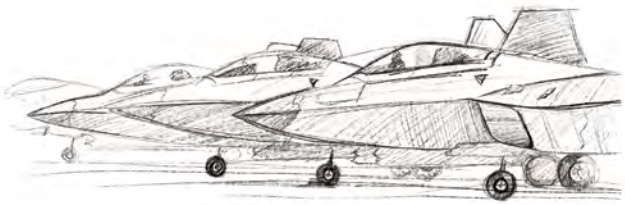
On a cold December evening in 2023, a retired U.S. Air Force pilot was finishing dinner with his family in their cabin on the James River near Norfolk, Virginia.

Through the windows he noticed unfamiliar lights floating in the night sky over the water. The blinking objects flew low, slow, and deliberately. One after another, the lights seemed to drift over the nearby Air Force base.

The lights weren't from any aircraft he recognized.

For the next seventeen days, similarly-lit objects were reportedly observed over Joint Base Langley–Eustis (JBLE). Night after night, there were dozens of sightings over restricted airspace at a base that is home to some of the U.S. Air Force's most advanced aircraft—the F-22 Raptor jet.

These reported objects did not attack. They caused no damage. Yet, their effect was unmistakable. They forced the relocation of F-22 Raptor jets responsible for homeland defense.



Seventeen days is a long time. Yet, this reflects how difficult it can be to detect and identify small aircraft operating in complex airspace.

More importantly, it took seventeen days for the base to determine what to do about the threat.

The uncertainty during those seventeen days reflects a sobering reality. It takes more than mere capability to protect against potential drone threats. It takes effective processes and pragmatic routines.

This event was not the first nor will it be the last incident where reported drones are seen unsettlingly close to military installations, communities, or critical infrastructure. Each sighting has triggered concern and raised questions. They remind observers of an uncomfortable truth—the skies are no longer predictable spaces. They require vigilant overwatch.

The response after the JBLE incident was typical. "Experts" called for better equipment to jam, shoot, or capture drones. They weren't necessarily wrong. But they overlooked the bigger picture—remember the 4 Ps discussed in the previous chapter?

In most security scenarios, it is a mistake to narrowly focus on defeating drone threats. Often the most valuable outcome is not, in fact, destroying the drone. Other outcomes are more valuable, including preventing, denying, containing, or diverting drone attempts, as well as attributing them to an operator.

Indeed, once a drone is overhead, the most important decisions about protection and countermeasures have already been made or, as it were, missed.

Thinking about the drone threat in these terms means considering the 4 Ps—the person, platform, process, and payload. At this point, you can start designing a set of resources and practices that buy time, deny value, clarify decision-making, and mitigate risk.

"Know thy enemy," the Chinese war theorist Sun Tzu said. Wise advice.

THE FIVE Ds OF DRONE PROTECTION

Good protection against drones isn't a well-aimed shot in the heat of an attack. It consists of smart actions taken by defenders before a drone launches, during its flight, and after an attempt has been made.

These actions aren't advanced or highly technical. They rely on several basic principles that you've probably applied when securing your house over the holidays while you're out of town on a family vacation. They are also fundamental principles used by the U.S. military, federal agents, and local law enforcement to protect assets on the ground. The sky, like a road or river, is just another route to your space.

These principles are guided by a few practical questions—questions defenders have always asked regardless of the threat or domain. First, how can I see trouble coming as early as possible? Second, how do I mess up my attacker's plans? Third, how do I convince an attacker to turn back because things are too risky or difficult? Fourth, what is my last resort to stop the threat? Finally, how do I ensure I stay cool and effective when things get crazy?

HOW CAN I SEE TROUBLE COMING AS EARLY AS POSSIBLE?

In any real-world security situation, having time to act is critical. While there is no crystal ball into the drone threat, there are ways to detect drones early. This can alter outcomes completely.

With drones, effective detection begins long before the drone even leaves the ground. It starts with understanding the threat environment. Who might target you? Why might they do so and how? Here are the 4 Ps again!

It is also about understanding yourself.

Whether you're in a convoy transporting critical supplies to a unit on a battle front, a technician working at a grid substation in a city suburb, or a homeowner with expensive equipment parked in the driveway, there are things about you that might attract nefarious attention from above.

Bad guys interested in information, attention, or violence tend to target things like critical infrastructure (power stations or transportation hubs), large gatherings (stadiums or markets), symbolic locations (government buildings or tourist attractions), high-value things or people, and sensitive security sites (military installations or prisons). They may use drones to surveil, disrupt, or attack any of these.

Knowing how you might attract interest is key, and it is the first, and most basic, form of detection.

Early detection is also a function of geography. The farther out you can see, the more likely you are to notice a threat—and have time to react—when danger is present.

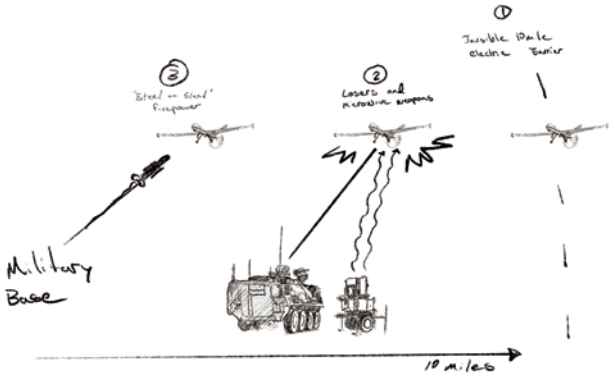
If you are securing your home against burglars, you want to know when someone suspicious walks up your road or driveway. This is why more and more homeowners have bought Ring cameras, providing 24/7 watch of their residences and properties. But drones are faster and more discreet than a person on foot, and they are difficult to deal with when they are already overhead.

To counter drones effectively, you must look beyond your immediate perimeter and consider the full 4 Ps of the drone threat ecosystem—not just the platform, but also the operator's location, method of control, and intended payload. This means assessing where an operator could maintain line of sight, conceal a ground control station, park a vehicle unnoticed, or launch drones from nearby rooftops, hilltops, or open fields. This process, known as "red teaming," involves thinking through an adversary's logic so you can anticipate vulnerabilities and take steps to prevent an incursion.

Sensing technology can also be a part of your protection plan. Drones can have identifiable silhouettes, produce recognizable sounds, emit predictable communication signals, and reflect energy. Monitoring devices can help you pick up on those cues. But, like driver-assist systems on cars, sensors shouldn't be completely counted on. These technologies have strengths and weaknesses. While some cars can back into parking spaces on their own, for instance, they sometimes make mistakes, which can cause accidents.

Drone detection relies on several complementary sensing methods. No single detection method—even the most high-tech—is sufficient on its own. They work together not to create perfect certainty, but to create decision-grade confidence.

Radar emits radio waves and analyzes their reflections to determine an object's distance, direction, and speed, allowing it to detect even silent or autonomous drones, though such systems are often complex, costly, and regulated. Optical and infrared cameras identify visual or heat contrast to confirm and track suspicious objects while acoustic sensors recognize the distinctive sounds of drone motors and propellers to provide limited early warning. Radio frequency detection intercepts signals between drones and their operators, sometimes revealing the drone's type, path, or operator location. Together, these tools vary widely in cost and capability but form the foundation of counter-drone awareness.



Offenders adapt to countermeasures—for instance, by reducing heat signatures, avoiding radio transmissions, or changing up preprogrammed routes. Detection works best when technical tools are layered with other protection practices: maintaining situational awareness and observing the environment, posting guards, conducting patrols, and collecting tips from the community.

When you have thought about the threat, assessed your own vulnerability, and layered methods for drone detection, you will be more likely to recognize when something doesn't seem right.

The goal of detection is not to prevent every attempt outright. It is to create time: time to understand, time to prepare, time to decide, and time to shape what happens next.

HOW DO I MESS UP THEIR PLANS IF THEY ATTACK ANYWAY?

While denial is probably the most overlooked step in drone defense, it is often the most effective step in protecting against drones.

Drones are flown for a reason. Some of the reasons are harmless like taking photos for a real estate ad. Some reasons are nefarious like conducting surveillance or conducting an attack.

Denial simply means keeping the operator from achieving some goal by complicating the effort. In practice, denial means taking away what the drone is trying to see, reach, or exploit. You can deny a drone's attack, for instance, even if it completes its flight.

To illustrate this simple but powerful idea, let's go back in time to World War II.

The newspapers were filled with tragic headlines and sobering photographs. Bomber planes were tearing through factories, rail yards, and city centers

across Europe and Asia leaving communities terrified and important infrastructure razed.

Americans grew concerned that it was only a matter of time before the war brought such destruction to the United States. As a result, leaders worked to protect key assets.

Just south of Seattle, Washington, stood Boeing Plant 2, a vast industrial complex producing the iconic B-17 and B-29 bombers, the backbone of American airpower. To enemy aircraft, it was a perfect target, if they could find it.

With help from Hollywood set designers, the U.S. Army Corps of Engineers constructed an elaborate deception canopy over the factory. From the air, what had been a sprawling industrial complex now looked like a quiet suburban neighborhood. Warehouse rooftops were disguised as houses. Netting was shaped and painted to resemble tree-lined streets, sidewalks, and yards. Even laundry appeared to hang in backyards.

To enemy aircraft, there was nothing to see. Nothing obvious to target. No anticipated payoff.



Today, denying drones may look a little different in form, but in practice it serves the same function.

Adversaries often use drones against critical infrastructure, crowded gatherings, symbolic locations, high-value people or assets, and sensitive security sites, so effective defense begins by denying them clear or attractive targets. This can involve dispersing crowds, vehicles, and equipment so they appear less meaningful from above, obscuring potential targets with clutter, camouflage, or structures that disrupt lines of sight, and deceiving operators through decoys, false electronic signatures, or misleading layouts designed to confuse what they see.

In essence, denial is about annoying, confusing, frustrating, or disappointing drone operators by making yourself uninteresting, uncertain, or unseen.

HOW DO I MAKE AN ATTACKER TURN BACK BECAUSE THINGS ARE TOO RISKY OR DIFFICULT?

Disruption accepts that a drone may still fly and focuses on making that flight risky or difficult.

Most drones rely on a combination of predictable hardware and software components, as discussed in Chapter One. Disruption introduces a little chaos into that picture. It forces the operator to change plans, make decisions under pressure, or doubt the chance of success.

Sometimes, you can accomplish disruption through detection and denial. As we mentioned in the section about sensors, things like RF (radio frequency) detectors and effectors can disrupt drone communications. Obscuring targets, a type of denial, can also disrupt a drone's flight plan by making it maneuver into vulnerable spaces or stay aloft longer than desired.

Two proven ways to disrupt drones are shaping their physical environment and interfering with their signals. Obstacles such as fencing, netting, or overhead structures can alter flight paths, block common avenues of approach, and push drones into visible or unfavorable routes while also degrading control links, GPS (Global Positioning Systems), or navigation timing. In

addition, many drones rely on RF communications or satellite navigation, so introducing interference or uncertainty into those signals can be enough to delay, confuse, or prevent the mission without destroying the aircraft.

Like detection and denial, disruption is not a standalone solution, but works best when it is integrated, rehearsed, and combined with other measures. Each layer complicates your opponent's plan and slows the attempt down.

WHAT IS MY LAST RESORT TO STOP THE THREAT?

Defeat is neutralizing the drone threat.

Of course, this is an important step. It is also probably what most people think of when they hear "countering drones." Paradoxically, it should also be the last of several steps you've taken.

Effective drone defeat means protecting what matters while limiting collateral damage. Defenders must therefore position counter-drone tools, or effectors, where they can act quickly enough to prevent harm without endangering people, infrastructure, or nearby airspace. In practice, there are four common defeat mechanisms, and the appropriate choice usually depends on the drone platform and its process of command and control.

First, drone defeat can occur through several mechanisms that target how the system functions. Link disruption uses jamming to degrade or break the control connection between a drone and its operator, often forcing the drone to hover, return home, land, or become too difficult to pilot, though fully autonomous drones may be less affected.

Second, navigation disruption employs jamming or spoofing to confuse GPS-dependent positioning, which can cause drifting, loitering, or mission failure—sometimes limiting the drone's behavior enough to support other countermeasures. Third, software disruption targets the surrounding system, such as the operator's device, applications, credentials, or data

links, denying reliable control or preventing the drone from achieving its intended result.

Finally, when immediate removal from the air is required, kinetic defeat provides a hard-kill option. This can involve intercepting drones with other aircraft, using explosives or directed fragmentation, capturing them with nets, or physically striking them by other available means. While often effective, kinetic methods carry higher risks of collateral damage, making careful consideration of the environment and safety of civilians essential.

Counter-drone techniques can be applied using a range of effectors, from low-cost and non-kinetic to high-tech and kinetic, depending on the target and threat. For example, protecting a critical target from a sophisticated drone with minimal collateral risk may call for an advanced kinetic effector to shoot or destroy it, while defending a less important target against a common drone with higher collateral risk might favor a low-cost, non-kinetic option like jamming.

As you can tell, the choice of a specific defeat mechanism depends largely on what the threat is. This means it is vital to gather as much information as possible on a drone during the detection phase. Detection will help you determine which of these defeat options is likely to work, when they can be applied safely, and how you confirm if they worked. Once you know what the drone depends on—link, navigation, autonomy, or an operator ecosystem—the menu of sensible options narrows quickly.

Each method carries different costs and risks, but the goal is the same. Protect what matters. Minimize unintended effects.

Most of the tools above are highly-regulated, available to the U.S. military and law enforcement, but not private individuals. You cannot, for instance, buy a jammer at Home Depot and use it for your home. While you can defeat a drone kinetically using a rifle or shotgun, it is difficult because some drones are small and fast. More importantly, it is often illegal for a private individual to shoot down a drone.



If you are doing small-scale drone defense, this means the other protection steps—detect, deny, disrupt—are your bread and butter. It also highlights the importance of understanding the laws that govern drone defense and the authorities held by you and your team to protect assets.

Generally, you should reflect on each interdiction of a drone to better know the adversary. In some cases, disabling a drone without destroying it can be just as valuable as bringing it down. Recovering a system may reveal who flew it, how it was controlled, and what it was meant to accomplish. That information feeds back into detection, denial, and disruption, strengthening your drone protection plan over time.

Like the other steps, defeat should be understood as part of a multi-step process and not your only focus. In most cases, successful protection means defeat is rarely required.

HOW DO I MAKE GOOD DECISIONS UNDER UNCERTAINTY?

Discipline is what allows everything else to work. It is the mindset that turns principles into action.

Protecting against drones almost always involves ambiguity. Identification

may be incomplete. Intent may be unclear. Safety concerns and collateral risk are real. Discipline is the ability to act deliberately under uncertainty.

In practice, discipline starts with clarity. Clear rules of engagement or use-of-force guidance. Clear authority to act. Clear understanding of who makes which decisions, under what conditions, and in coordination with whom. When those questions are unresolved, hesitation fills the gap.

Discipline also means knowing what "right" looks like before the moment arrives. Teams must understand what normal air activity looks like in their environment, what anomalies matter, and how information flows once something is detected. Who reports what? To whom? How quickly? What actions follow?

Discipline reflects the familiar measures long practiced on the ground to evade an adversary: noise and light discipline, cover and concealment, dispersion, movement. What changes is perspective. The enemy is no longer only across the street or beyond the ridgeline. They may be looking down and from a distance. Discipline now requires the willingness to alter routines, layouts, and behaviors with the assumption that observation can come from above and far away.

Discipline also requires preparation: rehearsals, battle drills, and tabletop exercises. Training helps teams recognize drone activity, understand what to report, and how to respond. In many environments, discipline also means coordinating beyond a single organization. Airspace is shared. Actions may require synchronization with law enforcement, local authorities, facility managers, or neighboring units.

Discipline is what builds awareness, shortens response times, and sharpens decisions.



THE NETWORK AS A TOOL

Now, imagine you are texting your friend on the phone and walk into an underground parking garage. It takes a few minutes to locate your car, back out of your spot and make your way up out of the garage. As you pass under the gate arm and emerge into the sunlight, your phone chimes and then chimes again.

You look down at your friend's message. "Hello????"

It's annoying when the network drops and you are in the middle of something, such as an important conversation.

When drones are inbound, you have seconds, not minutes, to react. In this case, a degraded network can be fatal, even if you have taken the drone protection principles seriously.

When protecting against drones, the network is your environment and it's just as important as having lights overhead or clear skies (we talk more about the environment in Chapter Five). You might feel ready to detect, deny, disrupt, and defeat adversaries. But if you can't track the drone quickly enough, it may not matter much.

When designing your drone protection plan, expect problems with your network. Think about how you will communicate with people and make important decisions even if the network drops. Think about what data should be prioritized if there is suddenly limited bandwidth. Having a PACE (primary, alternate, contingency, and emergency) plan for network connectivity is just as important in counter-drone operations as it is for communicating during a patrol or raid.

When protecting against drones the network matters. It matters a lot. A drone engagement is a race. Every unnecessary handoff, every extra screen, and every unprioritized video stream concedes seconds—and seconds can mean the difference between success and failure.

The seventeen days at JBLE were a wake-up call. They forced a return to the basics and a recognition that protecting against drones requires the steady application of familiar principles. With these principles in mind, including appreciation for the network, the next chapter discusses what protecting against drones may look like in practice.

Intentionally Left Blank

Chapter Four

The Five Ds in Practice

It is 0217 Zulu on an operations watch floor at a base somewhere in Kuwait, which was stood up following the start of Operation Epic Fury.

The Soldiers and Airmen on shift are doing normal things—drinking energy drinks and watching screens. Same landscape, different views.

One screen shows a video feed—a narrow band of desert road beneath a clear horizon. Another shows a map with a shaded trapezoidal shape plotted on top of it and labeled "defended zone." A third shows a clutter of applications and programs—chat boxes with operations discussion and intelligence reports, and boxes with scrolls of sensor and effector data.

The first indication of a drone threat doesn't come from the video. It is a dot on the map. Weak but stubbornly consistent. It appears, drops, and appears again. Initially, this flicker starts discussion across the watch floor. Quickly, this discussion turns into arguments. What was that? Was it something important? Was it a bird? Was it an error?

Meanwhile, the watch floor officer-in-charge does not announce a crisis. Instead, she does something more consequential. She coolly directs activity.

"Can you cue that sensor?" Then, she asks another Soldier to "turn on that screen to see if we can get another view."

The team does as she directs, waiting for her to determine whether the track is "real enough" to engage. They do these things calmly, as they've practiced many times before, almost anticipating what the officer-in-charge would ask next. Nothing dramatic. No alarms. Just a quiet (and boring) shift from routine to attention. Discipline in action.



It could have easily been missed—most newbies would have missed it. The blip on the screen didn't look like a drone. It looked weird but not dangerous.

A useful way to think about this is to ask a deceptively simple question: what does it mean to protect against drones?

PROTECTING AGAINST DRONES IS AN OUTCOME, NOT A MOMENT

As we've established throughout this book, protecting against drones is not a single action. It is a set of actions, driven by principles, taken when sensible, to achieve outcomes.

Effective protection is not cinematic. No Chekhov from *Star Trek* shouting, "but sir, the shields are down!" It is a subtle change in pressure from "something might be happening" to "we must act right now," and consists of logical, purposeful follow-through. Such disciplined reactions are where missions are saved or lost.

In many cases, dealing with the drone itself is the easy part. The hard part is everything around it—ensuring permissions, keeping people informed, anticipating changes in the environment, and managing your emotions. Finally, remembering that uncertainty and operating a bit on instinct is normal and doesn't signal failure.

In Chapter Three you learned the steps of protection—detect, deny, disrupt, and defeat, all underlined by discipline. But how do you put these principles into practice?

When the stakes are high, operations tempo fast, identification uncertain, and the risk vague, how do you put all these pieces together?

BUY TIME (GET "LEFT OF LAUNCH")

A drone in the air is not a spontaneous event.

Every drone is built, maintained, and prepared by its operator, who chooses launch sites, charges batteries, secures payloads, and tests control links. Effective defense requires taking the initiative by observing your surroundings—monitoring likely launch areas, tracking normal radio frequency (RF) activity, correlating drone sightings with time and traffic patterns, and distinguishing between harmless nuisance drones and more malicious threats.

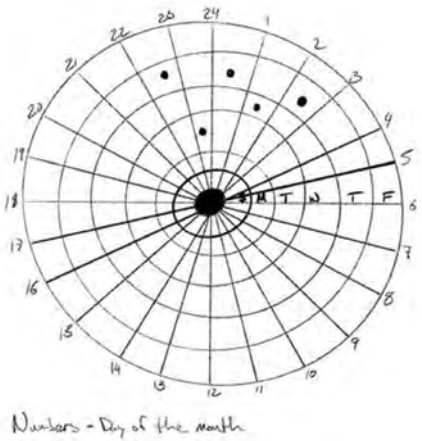
But remember—don't go overboard.

There is no need to become unnecessarily suspicious of your environment. Looking for patterns allows you to better see anomalies and predict your opponent's behavior. Knowing patterns buys time and allows you to go on the offensive.

Again, a drone in the air is not a spontaneous event. It has a supply chain. It has routines. It has patterns. Even the most improvised operations produce repeatable behaviors, because humans who operate drones are subject to re-

peat actions over time. The adversary's advantages, discussed in Chapters One and Two, create a vulnerability. When it is easy to try, it is easy to try again. When people try repeatedly, they leave patterns behind that are possible to predict—this is called pattern-of-life.

Prediction affords time, which is the real currency when protecting against drones. It allows you space for understanding and decision-making as you go through the sequence—detect, deny, disrupt, and defeat, all enabled by discipline. Effective detection isn't measured in distance from the threat, it is measured by the number of seconds you have to do something meaningful.



TEAMWORK MAKES THE DREAM WORK

Depending on your situation, you might find that the most expensive part of defending against drones isn't high-tech countermeasures. Rather, it's the team needed to address the drone threat.

Good prevention, especially in high-risk situations, can take a lot of operational management, especially of airspace and risk—both to force and mission. Managing those tasks means redirecting attention away from other tasks.

It is critical that you define who manages what and that you have the right team in place to tackle the complexity of the drone threat. Protecting against drones isn't the task of one person or a specially trained team. It is everyone's responsibility.

Sometimes the most likely drone targets are those that don't typically manage security—supply offices, medical facilities, or fuel stations. If you are a potential target (and you probably are), then know the basics to detect, deny, disrupt, and defeat, all shaped by discipline.

Remember, just because a drone isn't targeting you doesn't mean it's not targeting your operation. Reacting quickly and smartly, with discipline, could mean saving your team, if not yourself. Maintain logs and communicate so everyone knows that "the third incident this week" should be treated differently than "the first incident this month."

In short, drone protection takes teamwork.

PRACTICE MAKES PERFECT

Talking through what you could do (or would do) is a good first step to protection. What's the next step? Get out and try it. What seems simple on paper is, in fact, a tall order to exercise in real life. Not all anomalies are drones, and not all drones are threats.

Once you've thought through the 4 Ps and designed your detection plan, practice it. Test out your sensors to see what "strange" looks like. See how many views you need of a threat to have a complete picture. Practice identifying drone platforms, their command and control, and what payloads they may carry, which will enable you to think through how you'd react. Watch for flight profiles and drone behaviors—see how different profiles and behaviors change your reaction. You could easily draw on simulations to replicate drone behavior before going to the range. Drones must be woven into every field training and live-fire exercise, too, becoming as habitual as going to the rifle range.

In Monty Python's classic skit, "How Not to Be Seen," we learn that the first lesson of not being seen is not to stand up. Though resoundingly wise advice, hiding and camouflage do take a little more finesse. As established in Chapter Three, one of the most effective protection steps against drones is denial. Effective denial requires testing and adjusting your techniques. Practicing denial techniques during field training and live-fire exercises means working on camouflage—blending art and resourcefulness to make the things that matter blend into the landscape (like the Boeing Plant 2).

You should also familiarize yourself with and test your non-kinetic and kinetic effectors. Practice your protection techniques against realistic drone threats; incorporate different constellations of drone platforms, controlled by different connections, and require them to move along different avenues of approach with different payloads. Ukraine's success against Russian drones, for instance, was a function of trained operators capable of simultaneously coordinating many interceptors. Such practice might expose sobering lessons. Your jammers may have limited range, nets might have difficulty catching drones, shotguns may be useless, and rifles may have a hard time hitting drones at night.

In October 2025, the U.S. military conducted a joint, operational, and homeland defense exercise at Eglin Air Force Base in Florida, which was designed to assess the effectiveness of existing counter-drone capabilities against a range of realistic threats. The results allowed military leaders to understand gaps and limitations, therefore informing capability development, and demonstrated that all of us—Soldiers, federal agents, and local law enforcement officers—have a role to play in protecting against drones.

What made the exercise unique was the realism. Such realism and rigor should be the standard for training. The threat scenarios provided a realistic depiction of evolving adversarial drone operations. The scenarios consisted of different drones, ranging from small to medium to large, and multiple aerial axes of advance and threat profiles. This included a single drone, single axis incursion to a multiple axis, mass drone swarm incursion.

The threat scenarios were also informed by adversarial command and control covering a wide spectrum of emerging practices, including RF, fly-by-waypoint, fly-over-data, and first-person-view via fiber optic cabling. Though fiber optic drones circumvent many countermeasures, as reflected by Iran's and Russia's use of these capabilities, the exercise suggested that Ukraine's integration of multiple detectors—including acoustic sensors, computer vision, radars, and LiDAR (light detection and ranging)—can provide targetable tracks. These tracks can then que a layered defense, consisting of lasers, intercepting drones, small arms, and nets, to neutralize fiber optic drones.

Finally, like this exercise, the goal should be to repeatedly practice your drone protection procedures—in different environments, with different constraints and limitations, and when performing different missions. Who makes decisions? Is there someone you must call? How do you keep everyone alert to what is going on? This will help you navigate the requirement of communicating and collaborating under pressure, especially with Interagency partners. Federal agencies and departments of the U.S. government have unique authorities to engage drones in the homeland, for instance, which should inform your training, planning, rehearsals, and operations.



IT ALL COMES DOWN TO DISCIPLINE

Discipline is key in protecting against drones. The discipline to stay alert, stay up-to-date, and practice your procedures. It gives you the muscle memory to turn principles into action when things get exciting. In other words, discipline is what builds awareness, shortens response times, and sharpens decisions.

But how do drone defenders build discipline?

First, stay aware and alert by understanding what normal air activity looks like in your area, recognizing unusual or concerning anomalies. Know which anomalies matter, how to gather information when uncertain, and the proper reporting process—who reports what, to whom, how quickly, and what actions follow. Also, be clear on who else needs to be informed, such as law enforcement, neighboring sites, or the public.

Second, know the rules of engagement for drones, including when and how force can be used. Be aware of who is authorized to make response decisions and under what conditions, and ensure you understand the law and the limits of your authorities.

Finally, regularly rehearse potential threats by practicing how to detect, deny, disrupt, and defeat drones, building anticipation for emerging dangers. At the same time, maintain discretion by avoiding drawing attention to critical assets, concealing what matters—including yourself and your team in high-risk areas—and varying your activities and routes to remain unpredictable.

WHAT SUCCESS LOOKS LIKE

The shift does not feel frantic. The watch floor is not drowning in alarms. Operators are not improvising responses. When a drone appears, it is often already "expected," in the sense that the environment has a baseline of drone

activity and deviations are quickly recognized. The response is proportionate—selective, disciplined, and repeatable. The event does not necessarily end with a dramatic defeat; it ends with continuity.

That kind of success is easy to miss because it is not theatrical. It looks like nothing happened.

But that is the point.

Protecting against drones, properly understood, is not a contest of fear. It is a contest of time, structure, and repeatability. Left of launch is where time is easiest to buy since the best defense is often a good offense. Threat understanding is how you spend time wisely. Denial, disruption, and defeat are what you do when prevention fails.

If you measure only the moment of impact, you will always feel behind. If you measure how often the adversary's attempt fails to produce an effect—how often they are deterred, disrupted, contained, or forced into predictable patterns—you begin to see the problem for what it is: a practical challenge of systems design and disciplined operations.



The track on the screen at 0217 Zulu eventually resolves. It becomes real enough. The second sensor confirms it's an adversary drone. The watch lead makes a call that has been rehearsed and authorized, and the posture shift again—quietly, in time.

Nothing about the response requires magic. It requires something better: a team that has treated protection as an operational craft, not a crisis. And when that is true, the enormity of the counter-drone problem shrinks into a manageable detail. But this requires us to adopt a new appreciation of the terrain of protecting against drones, and artificial intelligence, which we explore in the final two chapters.

Intentionally Left Blank

Part III: Key Considerations

Protecting Against Drones in New Terrain
What is Role of Artificial Intelligence?

Chapter Five

Protecting Against Drones in New Terrain

The map is simple enough.

The defended zone is outlined with a polygon—critical infrastructure and high-value assets fit neatly into the outline with neat crosshatching to shade the area. The area of interest is a bubble around that, shaded more lightly. On the map on the screen, icons are placed in orderly lines on hilltops to show where there are sensors—radars, cameras, acoustic microphones and radio frequency (RF) detectors. By the looks of it, nothing is getting by this baby.

The briefing ends, the laptops close, and the team of federal agents heads to the site.

At a parking lot, the federal agents park and hop out of their trucks. They are on the edge of town where the cityscape squeezes up against the mountains. On one side of the parking lot there is a tidy apartment building and a warehouse just beyond that. On the other, a craggy hillside covered with tall grass, blackberry brambles, and the occasional oak tree.

The team trips and scrambles up the hillside—which on the map was a cluster of topographic lines. The wind picks up the higher they go. A welcome respite from the heat.



At the top there are bushes and long grasses bending in the breeze. The valley below shimmers with the heat of the town; sunlight bounces off the metal roofs and street signs. There is a rusted metal structure on the hill—maybe the legs of an old water tank. It seems an obvious spot to mount equipment, but of course the cell signal is crap. There were plenty of bars in the parking lot.

One agent pulls out a chunky looking tablet to check out the RF signals in the area. The warehouse they'd seen below must be some kind of manufacturing operation. It's pumping out electromagnetic interference, maybe from a fan or conveyor belt motor.

That didn't show up on the PowerPoint slides.

And, go figure, the network connection was bad. On the plan it looked like a straight line, but with so many obstacles they were going to need to hop between multiple routers and switches with limited bandwidth.

You know what they say about best-laid plans.

I DON'T UNDERSTAND— THIS WAS WORKING BEFORE

Stud finders. What useful tools.

You slide one across a wall, and it beeps and lights up when it's found the wooden stud behind. That way you can be sure that the nail you're using to hang your grandma's portrait is hammered into something solid rather than flimsy drywall.

But when you slide it across the living room wall in your old, four-times remodeled house, it doesn't beep at all. You slide it again and it flashes briefly, then flashes again. Is that a stud? And another 6 inches to the right? That doesn't make sense! Finally, you resort to frustrated knocking to see if you can determine where the wall is hollow or solid.

I don't get it. "Why did it work there but not here?" you ponder.

By analogy, this is the one question that drone operators and defenders ask all the time, usually with a mix of frustration and disbelief. "Why did my equipment work there but not here?" Usually, the first thing they do is blame the equipment. They assume a device is too cheap, and the guy who sold it was a con artist.

But in a surprising number of cases, the system performed as well as it could have, given the physics. The problem was not the device. The problem was the terrain.

When we talk about the environment, we usually mean the physical environment—plants, hills, buildings, etc. In terms of drone protection, the environment includes two additional "spaces"—the electromagnetic spectrum and network.

HOW CAN THE PHYSICAL ENVIRONMENT AFFECT DRONE PROTECTION?

The physical environment significantly influences both drone operations and defensive measures. Landscapes like hills, mountains, and ridgelines provide natural cover, allowing drones to approach unseen, while urban areas let them

slip between buildings, cars, and other clutter. At the same time, features such as buildings and terrain can obstruct radio and network signals, limiting line-of-sight communication between drones and operators.

Environmental features also create signal reflections and interference, complicating detection. High-rises, metal roofs, warehouses, and fences can make radio waves behave unpredictably, producing echoes or "ghost" signals that distort direction and strength readings. Trees, leaves, and branches absorb and scatter higher-frequency signals while wind and weather—rain, fog, snow, heat shimmer—further alter radio and light propagation. Infrared detection is similarly affected, as sun-heated surfaces like rocks, asphalt, and metal can create false heat signatures, making it harder to distinguish drones from the background.

These environmental factors can shorten drone ranges, make operations unpredictable, and reduce detector reliability. Drones may appear to lose links unexpectedly behind obstacles, or defenders may perceive them coming from misleading directions. Much like the inconsistent cell reception we experience daily, these small environmental effects compound when seconds matter in drone defense. The key is to recognize and account for this complexity, avoiding wasted time on false signals or overreliance on imperfect detection systems.



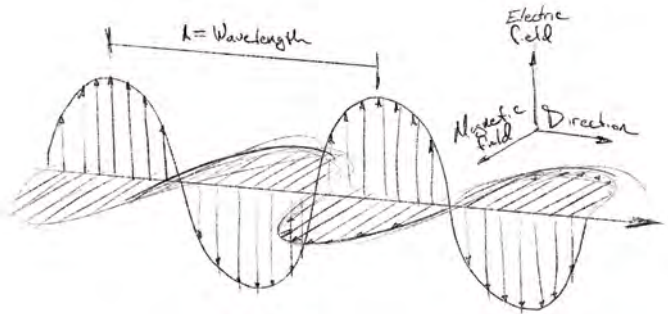
HOW CAN THE ELECTROMAGNETIC SPECTRUM AFFECT DRONE PROTECTION?

The electromagnetic spectrum (EMS) also shapes how drones operate and how they can be defended against. It encompasses all energy waves passing through the air, from radio and microwaves to infrared, visible light, ultraviolet, X-rays, and gamma rays, each at different frequencies describing how many wave cycles pass a point each second.

For drone operators and defenders, the spectrum acts like a physical environment that the drone moves through. Data links between the operator and drone rely on specific frequency bands, typically 2.4 GHz and 5.8 GHz for Wi-Fi and commercial chips, or 700 MHz–2.4 GHz for 4G and 5G cellular networks. Relays can extend these links, while congestion or interference on the same band can slow responses, drop data, reduce range, or drain batteries.

Another key factor is the noise floor—the baseline of electromagnetic energy from electronics, routers, machinery, and other sources. Signal strength, measured in negative dBm values, diminishes with distance and can be drowned out by a high noise floor, just as a soft voice is lost in a noisy room. A strong noise floor can limit a drone's range, affect its data link, and even allow the drone to "hide in the noise," making it harder for RF detectors to identify. Understanding these patterns helps both operators maintain reliable connections and defenders anticipate where drones may go undetected.

By treating the EMS as part of the operational environment, alongside the physical landscape, defenders can better leverage environmental factors to protect assets. Just as hills, buildings, and trees influence visibility and movement, the EMS influences communications, navigation, and detection, providing opportunities to exploit interference, congestion, or noise to limit drone effectiveness.



THE BASICS OF JAMMING

Jamming drones is like creating a dense fog on a roadway—by injecting energy at a specific frequency or band, a jammer congests the spectrum, causing drones or equipment operating on that frequency to lag, drop video, return home, or abort their mission. A jammer raises the noise floor, targeting the drone's control link rather than the aircraft itself, and can operate wideband for broad coverage or narrowband for focused efficiency. Its effects vary, including loss of control, forced autonomy, or switching between connections.

However, jamming is not a predictable or guaranteed solution. Just as drivers navigate around traffic jams, drones may adapt by switching frequencies, regaining line of sight, or using alternate networks, meaning a jammer placed perfectly may still have little visible effect. This unpredictability highlights that jamming alone is rarely sufficient.

Effective defense requires understanding what the drone depends on at any moment. Defenders should identify the drone's dependencies—its control links, navigation signals, or data connections—and work to deny them, using jamming alongside other protection techniques to address as many vulnerabilities as possible.

WHEN ENVIRONMENTS COLLIDE

The simplest way to see the interaction among these three terrains—physical, spectrum, network—is to notice how often a drone "wins" without being sophisticated.

The drone flies low, using the ridgeline as cover. Physical terrain reduces detection. The operator tries to jam it, but the drone is already in a mode that does not depend on continuous control. It's flying semi-autonomously.

Spectrum terrain reduces effectiveness. The team tries to push video to a remote operations center for confirmation, but the link is congested and the video lags. Network terrain steals time. By the time the decision is made, the drone is past the point where any mitigation option is both safe and effective.

This is where the commercial drone ecosystem has quietly changed the fight. The defender's mental model is to "deny the drone's link." The drone's reality is "the mission continues on whatever connection dependency remains." If RF becomes unreliable, the control path may ride something else.

If the control path becomes intermittent, autonomy carries the last mile. As the connection paths shift, the defender's own system is tested—not just for capability, but for speed of adaptation.

In after-action reviews, this story is often told as a failure of a particular component of layered defense. The radar didn't see it, the jammer didn't work, the network was slow. The deeper truth is that the terrain was never modeled as a unified problem.

High-performing units appreciate this reality. They read terrain the way experienced aviators read weather—not as a surprise, but as a set of constraints to plan around.

They do not plan only with maps. They plan with modeled viewsheds—what can each sensor see from its position? They plan with RF propagation in mind—what links will work, where, and under what conditions? They plan with network pathing—how data will travel, what happens when a connection fails, what degrades, and what catastrophically breaks?



They also plan with humility. They accept that no plan will be perfect. They build for resilience.

Resilience is not a buzzword. It is a design choice. Local edge processing at the lowest echelon can function when backhaul fails. Layered sensing allows one sensor's blind spot to be filled by another sensor's strength; decision authorities allow local action when central confirmation is delayed; playbooks specify what happens when the network is degraded, when satellite jamming is unreliable, when spectrum conditions change.

For drone defenders, this changes how you think about sensor and effector emplacement. You are not placing sensors in isolation; you are placing a system across three terrains. The question is not "Where can I see?" It is "Where can I see, communicate, and act with enough time to matter?"

For senior leaders and staff members, the same logic changes how you think about investment. The question is not "Which sensor is best?" It is "Which

architecture produces decision-grade awareness reliably across realistic terrain and network conditions?" That question tends to reward integration, modularity, and repeatable deployment patterns—not one-off excellence.

The reason this reframing is important is that it replaces a vague sense of difficulty with a practical method. Terrain is not a monster. Terrain is a set of constraints. Constraints can be modeled. Modeled constraints can be planned against. Planned constraints can be trained on by teams, as discussed in the previous chapter. When teams do that, protecting against drones begins to look less like a chaotic contest of gadgets and more like a disciplined craft. This is a key principle of protecting against drones.

But what about artificial intelligence? Can it help resolve the challenge of protecting against drones in new terrain?

Intentionally Left Blank

Chapter Six

What is the Role of Artificial Intelligence?

The unit missed it.

Not because no one was watching. Not because no one cared. And, not because there were no warnings.

The drone was in the air long enough to matter. It loitered over the people the unit was charged with protecting. It was there long enough to raise questions. It was there long enough that the consequences could have been worse.

If only the unit had seen it sooner. If only the right sensor had been looking in the right direction. If only the report from the patrol had been connected to the anomaly someone else noticed on a screen. If only there had been enough people in the operations center to watch everything at once, to make the connections that might have informed a decision to act.

If only.



Inside the Base Defense Operations Center (BDOC), the conditions were familiar: multiple screens and feeds, camera views and sensor data, radar tracks appearing and disappearing, radio calls from teams on the ground, civilian air traffic overhead, and legitimate drones operating throughout the nearby city.

It was a flood of information. Each piece made sense on its own. None of it demanded action. The patrol that noticed something unusual could not be sure. The sensor that picked up a brief anomaly lost it seconds later. Another system flagged a track, then dismissed it as clutter.

No one was wrong. However, no one saw the whole picture. By the time the pieces came together, the drone was gone.

It didn't attack. It didn't have to. It gathered information. It tested reactions. It signaled vulnerability. All the outcomes that matter for the enemy as discussed in Chapters One and Two.

The question afterward was not *who* failed. The question was *how*? With all the tools, all the training, and all the information, *how* did the Soldiers miss it? *How* can they make sure it doesn't happen again?

ARTIFICIAL INTELLIGENCE HELPS

Artificial intelligence (AI) is not the final answer. Without it, teams will continue to miss things that matter.

There is a temptation to talk about AI as either a savior or a threat, either a magical solution that fixes everything or a frightening force that removes human control. Neither description is useful. In practice, AI is far more neutral than either of these extreme perspectives suggest.

Put simply, AI is a set of tools designed to help computers recognize patterns, learn from data, make predictions, and assist humans in making decisions,

especially when the volume of information exceeds what any one person or team can reasonably manage. It does not replace judgment and disciplined decision-making. It does not understand intent or consequences. It does not decide what matters. What it does well is sort, compare, correlate, and highlight signals that would otherwise be lost in the noise, as explained in the previous chapter.

That distinction matters, especially when protecting against drones. AI does not counter drones. People do. AI helps people do it better and faster. Planning software, sensors, decision tools, and effectors enabled by AI fuse and filter information, shifting advantage back to the defender by buying time, reducing overload, and helping humans apply the principles of detection, denial, disruption, defeat, and discipline more effectively.

CLEARING THE AIR

Most of what we call AI today is not a single thing. It is a collection of simple processes working together, quietly at speed and scale. To understand how AI supports countering drones, it helps to demystify what is happening behind the scenes.

At the foundation of AI are algorithms. These are sets of coded instructions that tell a computer how to sort, compare, and evaluate information. On their own, algorithms are not intelligent. They are rules. What gives them power is the data they operate on and the speed with which they can apply those rules again and again. Data and computing power allow algorithms to run millions of comparisons faster than any human could manage, without fatigue or distraction.

Machine learning builds on this foundation. Instead of being told exactly what a drone looks like, sounds like, or how it behaves, an AI decision support system incorporating machine learning is exposed to thousands or millions of examples. Over time, it becomes better at recognizing patterns and, even more importantly, when something breaks a pattern. In counter-drone

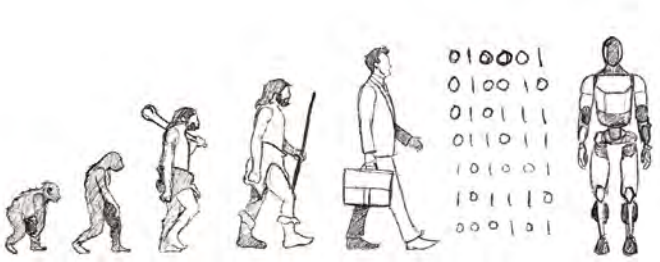
operations, that might mean learning to separate birds from quadcopters, background noise from propellers, or routine air traffic from something behaving just slightly differently than normal. The system does not "know" what it is seeing. It recognizes familiarity, notices deviation, and can flag anomalies.

Large language models (LLM) build on these same learning processes but apply them to language rather than sensor data. They do not think, reason, or understand intent. What they do well is organize information by summarizing reports, translating inputs, flagging inconsistencies, and helping people make sense of fast-moving situations. In a BDOC flooded with radio calls, text messages, and alerts, LLMs can help turn raw inputs into something readable and actionable. They do not replace analysis. They make analysis possible under pressure and fatigue.

All these processes depend on data—sensor feeds, imagery, radar tracks, radio frequency detections, and reports from people on the ground—and on computing power capable of processing all that data in real time. The quality of the output is shaped not just by the sophistication of the algorithm, but by the relevance of the data and the speed with which it can be processed.

Automation is what allows these systems to handle routine tasks continuously. Tracking objects. Updating displays. Cross-referencing reports. Cueing one sensor based on another. These functions are time-consuming but essential. Automating them does not remove humans from the process. It preserves human attention for the decisions that require judgment.

Autonomy is different. Autonomous systems can act independently or without human oversight within defined limits. When it comes to protecting against drones, that autonomy is rarely absolute. It is constrained, deliberate, and closely tied to assessments of risk, confidence, and trust. A system may automatically classify a track, recommend a response, or slew a sensor, while humans retain authority over actions that carry legal, moral, and ethical, as well as escalatory, consequences.



How much autonomy is acceptable depends on context. It depends on how credible the threat appears, how trusting operators are of a system's performance, how well the action aligns with rules of engagement and regulations, and how much risk the decision carries. Systems are trusted and granted greater freedom when they can show that they minimize civilian harm, maximize the protection of friendly forces, and contribute meaningfully to mission success. Where those conditions are not met, humans step back in.

In high-risk combat environments, greater autonomy may be necessary to keep pace with the drone threat, especially because drones are also increasingly outfitted with AI, as discussed in Chapters One and Two. In homeland protection settings, autonomy can be more limited, shaped by legal constraints and the need for human accountability necessary to reduce risks to civilians. In both cases, autonomy is not about surrendering human control. It is about managing time.

None of these elements are revolutionary on their own. What makes AI so powerful, so helpful, is how it integrates these elements to work together. Algorithms sort. Machine learning refines. Language models explain. Automation routinizes. Carefully bounded autonomy accelerates. The result is not a machine that replaces people, but one that helps them see connections sooner, prioritize more effectively, and act with greater confidence, before it's too late.

ARTIFICIAL INTELLIGENCE, REAL PROTECTION

When protecting against drones, AI is not only useful in moments of crisis, when stress is high in a BDOC or when a patrol is already reacting. Its value extends across the entire protection challenge, long before a drone poses a threat.

Long before launch, AI can help shape how defenders understand risk. Intelligence analysts already study terrain, past incidents, reporting, and open-source information to anticipate where threats may emerge. Artificial intelligence accelerates this work by fusing disparate data, flagging emerging patterns, exposing pre-attack indicators, and helping analysts identify which assets attract attention, which approaches are vulnerable, and where defensive measures are likely to matter most. Artificial intelligence does not decide what must be protected. It helps humans see where protection deserves priority.

As operations move closer to the moment of action, AI becomes even more consequential. Environments that require protection are crowded, contested, and complex. Airspace contains birds, helicopters, fixed-wing aircraft, and legitimate commercial drones. Threats are concealed within this background. Sensors are always watching, but they do not understand all that they see.

Data representative of this environment allows AI-enabled detection systems to learn what "normal" looks like in a specific place, at a specific time, and under specific conditions. When something deviates—slightly slower, quieter, more persistent, or out of place—AI can flag it earlier than humans scanning screens.

Detection, however, is rarely the job of a single sensor. Radar detects movement. Cameras reveal shape and heat. Radio frequency sensors listen. People on the ground notice and report behaviors that don't feel right. Artificial intelligence helps connect these fragments of information, correlating a ra-

dar track with a brief visual cue, linking a patrol's report with a signal that would otherwise be dismissed as clutter. The result is not perfect clarity, but greater coherence to enable engagement decisions.

Artificial intelligence also supports denial by informing where protection will be most effective. By analyzing sightlines, coverage gaps, terrain, and historical patterns, AI can help determine where concealment, hardening, deception, or sensor placement will have the greatest impact. It can suggest where to emplace protection measures so that drones struggle to see, reach, or exploit what matters most.

When a drone begins to behave like a threat, AI-enabled decision support systems can help humans decide what to do next. Drawing on sensor data, flight behavior, proximity to protected assets, known drone profiles, databases of friendly or authorized aircraft, and rules of engagement parameters, these systems can recommend courses of action. They do not decide. They advise, helping operators weigh options such as continued monitoring, electronic disruption, or physical defeat.

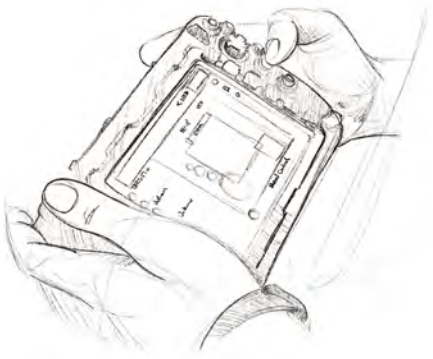
Disruption is where AI's value becomes more dynamic. Counter-drone operations often rely on interfering with navigation, communications, or control links. Artificial intelligence can help assess what type of drone is present, how it is likely being controlled, and how it is responding to interference. It can monitor whether disruption is having an effect and help operators decide whether to adjust or escalate.

When defeat becomes necessary, AI can still support human judgment. By modeling trajectories, estimating crash locations, and assessing collateral risk, AI-enabled systems help Soldiers choose where and when to act. In more advanced systems, AI supports interceptor drones by enabling navigation, target tracking, and timing at speeds humans cannot match, while keeping humans firmly in control.

After the drone is down or gone, AI continues to matter. Recovered systems, sensor logs, and operational observations are all forms of data. This data

feeds back into algorithms enhanced with machine learning to refine a system's future performance.

This is how AI helps to protect against drones. It does not promise perfect defense. It promises fewer blind spots, shorter delays, better prioritization, and fewer moments where the only explanation is that the pieces were there, but no one had time to connect them.



THIS TIME, WITH ARTIFICIAL INTELLIGENCE

There are reports of a drone and the conditions look familiar. The screens are still crowded. The airspace is still busy. Information still arrives in fragments.

This time, the anomaly is not lost in the noise. A sensor cues a camera. The camera confirms the report from the patrol. The track is clear. Soldiers' attention shifts earlier. The operators decide to respond in time for it to matter.

This time, they don't miss it.

Conclusion

Ending the "Happy Time"

The wind cut sharply across the ridgeline as a platoon from the U.S. Army National Guard settled into position somewhere in Kuwait just before dawn. It was there to help protect a U.S. military base from Iranian Shahed-136 drone attacks.

Frost clung to camouflage netting pulled low over vehicles. Radios stayed quiet except for brief, deliberate transmissions. What once might have looked like stillness was, in fact, preparation—every Soldier rehearsing the quiet habits of protection learned through months of disciplined training.

Then came the sound.

Not loud.

Not dramatic.

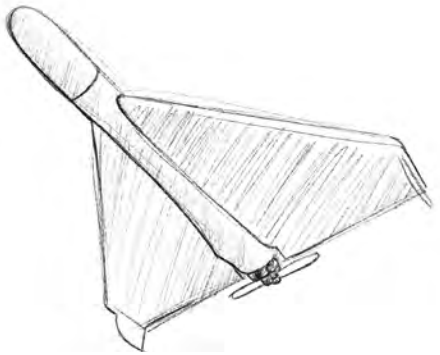
Just the faint mechanical buzz of a small drone somewhere beyond the next fold of terrain, similar to that heard during Ukraine's Operation Spider's Web.

No one panicked. No one searched the sky in confusion. A track had already appeared on a handheld display moments earlier—weak, intermittent, and uncertain, the kind of ambiguity the Base Defense Operations Center had learned to take seriously long before a drone became visible. A second sensor cued. A third confirmed. Within seconds, the platoon shifted posture: dispersion widened, thermal signatures reduced, observation oriented toward likely launch corridors shaped by the surrounding terrain.

Nothing about the moment felt cinematic.

Everything about it felt practiced.

"We used to look up and wonder what to do," one Squad Leader said quietly. "Now we look up and already know."



There was a time when this wasn't true.

Early in the proliferation of drone warfare, small unmanned aircraft systems enjoyed their own version of a "happy time"—a period when they were poorly understood, lightly contested, and disproportionately effective. Like German U-boats in the early years of World War II, drones thrived in the gap between innovation and adaptation. They were cheap, persistent, and psychologically disruptive. For a time, they dictated behavior.

But, like U-boats, they did not remain unchallenged.

Protecting against drones, small or large, is not a single dramatic engagement. It is the steady application of principles across time and space—detect, deny, disrupt, and defeat—bound together by discipline. Long before a button is pushed or a trigger is pulled, protection is already underway in pattern recognition, posture adjustment, and the quiet denial of useful information to an adversary.

As one Soldier explained, "If the drone never gets a clear picture, we've already won."

That is how the "happy time" ends - not with a single breakthrough technology, but through accumulated adaptation and innovation. Convoys replaced vulnerable shipping when confronted with U-boats. Most importantly, people learned. What was once novel became familiar; what was once feared became manageable.

Soldiers from the U.S. Army National Guard learned this lesson the same way professionals always do: through realistic training that replaces assumptions with understanding. They discovered that shooting down drones is rarely the decisive act. Detection and passive protection matter more. If a drone cannot find you, cannot track you, or cannot produce an effect, the mission fails regardless of whether the drone survives. Protection, as earlier chapters have made clear, is an outcome, not a moment.

"You don't wait for the threat," a Platoon Sergeant observes. "You shape the fight before it sees you."

Training is crucial to transforming how we think about protection. Infantry squads learn they are not just protecting themselves but forming the forward edge of a layered defense shielding command posts, artillery, sustainment convoys, and medical sites. Logisticians learn camouflage, dispersion, and emissions discipline are as vital as fuel and timelines. Rear areas and front lines fuse into a single system of collective protection—evidence that counter-drone defense is a team effort, not a specialty skill.

"One unit slipping up puts everyone at risk," a sustainment Sergeant noted. "Protection only works if we all do it together."

A new way of understanding terrain reinforces this approach. Maps promise clarity; reality imposes constraints. Hills mask flight paths. Urban clutter distorts sensors. Vegetation absorbs signals. Networks lag. Spectrum noise hides faint links. The battlefield extends vertically and invisibly into elec-

tromagnetic and digital space. Units that succeed may not have perfect equipment, but they succeed by honestly reading terrain—placing sensors, managing networks, and understanding authorities so information becomes actionable in seconds.

"The ground still matters," a young Lieutenant reflects, "but now we fight for the sky above it too."

Artificial intelligence adds another layer—not as magic, but as assistance. It helps identify faint patterns within overwhelming data, connect scattered anomalies, and warn humans early enough to matter. It reduces cognitive burden without replacing judgment. Properly used, it restores clarity in environments defined by ambiguity. The result is not autonomy, but awareness—faster, broader, and more actionable.

"The system gives us seconds," one operator explained. "Training tells us what to do with that time."

Taken together, these lessons reveal something more than tactics or technology. They show how adaptation and innovation unfolds. History repeats the pattern: uncertainty gives way to study, study to training, training to competence, and competence to confidence. The "happy time" ends not because the threat disappears, but because defenders learn how to live with it—and overcome it.

"You stop thinking about the drone," a Team Leader says. "You start thinking about the mission again."

This transformation is now visible across the Joint Force, federal agencies, and local law enforcement. Personnel who once reacted now anticipate. Units that once paused now continue the mission. Adversaries who relied on surprise increasingly encounter preparation. The sky has not become safe—but it has become understood, and understanding is the beginning of protection.

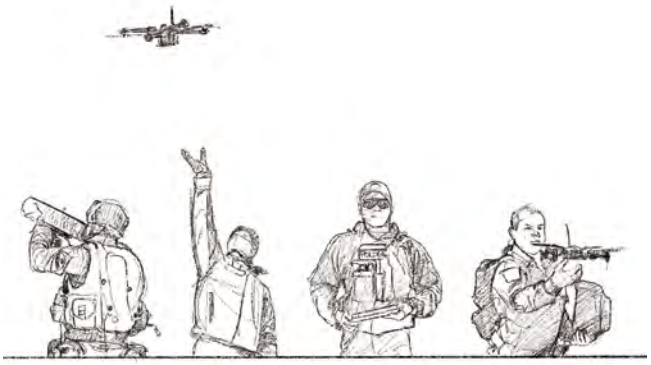
Drones will continue to evolve. Yet the foundation of protection—principles applied with discipline, shaped by terrain, strengthened by training, and accelerated by intelligent systems—will remain constant.

Defenders who master protection will meet future threats the same way the platoon met the faint hum beyond the ridge: prepared, ready, and unafraid.

The "happy time" of drones, like that of Germany's U-boats, was never permanent. It belonged to a moment—one defined by surprise, uncertainty, and inexperience. That moment has passed.

What remains is something far more enduring: adaptation and innovation.

This is what ends the "happy time" of new technologies, including drones.



Intentionally Left Blank

Appendix A

A Professional Glossary

Protecting against drones has developed a lexicon of terms and acronyms. Since this publication is a primer, it is intentionally written in plain language. However, preparing to protect against drones requires familiarity with certain terms and acronyms; they provide clarity and shared understanding.

The terms below serve as an introduction to this lexicon.

Adversary
A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

Artificial Intelligence
The ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action—whether digitally or as the smart software behind autonomous physical systems. (2018 DOD AI Strategy)

Automation
The creation and application of technology to monitor and control the production and delivery of products and services with no or limited manual tasks or activities. (DoDI 5000.94)

Autonomy
The level of independence that humans grant a system to execute a given task. It is the condition or quality of being self-governing to achieve an assigned task based on the system's own situational awareness (integrated sensing, perceiving, analyzing), planning and decision-making.

Autonomy refers to a spectrum of automation in which independent decisionmaking can be tailored for a specific mission, level of risk, and degree of human-machine teaming. (Joint Concept for Robotic and Autonomous Systems)

Command and Control
The personnel, facilities, equipment, communications, and procedures essential for a commander to plan, direct, and control operations of forces pursuant to the missions assigned. (JP 6-0)

Common Operational Picture
A single, identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness. (JP 3-0)

Defeat
The physical or functional neutralization of an unmanned vehicle so that it no longer poses a threat. This may include kinetic means, electronic warfare, capture mechanisms, or other effects conducted in accordance with lawful authorities. (Counter-Manned Systems Study)

Denial
Measures to remove or reduce the value of what the threat is trying to achieve—for example, obscuration, hardening, dispersion, or deception—that frustrate an adversary's ability to see, target, and strike. (Small Drones, Big Problems: A First Principles Approach to Countering-UAS)

Detection
The act of discovering the presence of a potential threat using sensors of observation. Also called identification. (Counter-Manned Systems Study)

Effect
The physical or behavioral state of a system that results from an action, a set of actions, or another effect. 2. The result, outcome, or consequence of an action. 3. A change to a condition, behavior, or degree of freedom. (JP 3-0)

Electromagnetic Attack
Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-85)

Electromagnetic Interference
Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. (JP 3-85)

Electromagnetic Protection
Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-85)

Electromagnetic Spectrum
The range of frequencies of electromagnetic radiation from zero to infinity, divided into 26 alphabetically designated bands. (JP 3-13.1)

Electromagnetic Spectrum Management
The operational, engineering, and administrative procedures to plan and coordinate operations within the electromagnetic operational environment. (JP 3-85)

Electromagnetic Vulnerability
The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of electromagnetic environmental effects. (JP 3-85)

Electromagnetic Warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called Electronic Warfare. (JP 3-85)

Emission Security
The portion of communications security designed to deny unauthorized persons information of value as a result of intercept and analysis of compromising emanations from cryptographic equipment and telecommunications systems. (JP 6-0)

Engage
In air and missile defense, a fire control order used to direct or authorize units and/or weapon systems to attack a designated target. (JP 3-01)

Interagency Coordination
The planning and synchronization of efforts that occur between elements of Department of Defense and participating United States Government departments and agencies. (JP 3-0)

Machine Learning
An application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed. (15 U.S. Code 9401)

Network
The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (JP 1-02)

Passive Defense
Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative. (JP 3-60)

Protection
Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and

infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 3-0)

Protecting against Drones
The deliberate effort to reduce an adversary's ability to use unmanned vehicles to observe, disrupt, coerce, or attack—before launch, during flight, and after an attempt has been made. (Small Drones, Big Problems: A First Principles Approach to Countering-UAS)

Risk
The probability and consequence of an event causing harm to something valued, classified within four risk levels—low, moderate, significant, high. (CJCSM 3105.01B)

Risk Management
The process to identify, assess, and mitigate risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

Rules of Engagement
Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. (JP 3-84)

Strike
An attack to damage or destroy an objective or a capability. (JP 3-0).

Surveillance
The systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. (JP 3-0)

Targeting
The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

Track
A series of related contacts displayed on a data display console or other display device. (JP 3-01)

Unmanned Vehicle
A vehicle, whether on land, sea, or air, that does not carry a human operator and is capable of operation with or without human remote control. (JP 3-30)

Vulnerability
The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 3-01)

Vulnerability Assessment
A Department of War, command, or unit-level evaluation to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a physical or cyberspace threat. (JP 3-26)

Weapons Control Status
An air and missile defense control measure declared for a particular area and time by an area air defense commander, or delegated subordinate commander, based on the rules of engagement that establish the conditions under which fighters and surface air defense weapons are permitted to engage threats. (JP 3-01)

Weapons Free
Weapons free is the least restrictive status. It is used to indicate when any target not positively identified as friendly in accordance with current rules of engagement may be engaged. (JP 3-01)

Weapons Hold
Weapons hold is the most restrictive status. Units may only fire in self-defense or when ordered by proper higher authority. (JP 3-01)

Weapons Tight

Weapons tight is the normal status. Units may only fire on targets identified as hostile in accordance with current rules of engagement. (JP 3-01)

Intentionally Left Blank

Appendix B

An Annotated Bibliography for Joint Doctrine

This publication is written for anyone's consumption. It is meant to provide a basic understanding of how personnel from across the Joint Force, federal agencies and departments, and local law enforcement protect against drones. It is just one of numerous documents that are intended to inform protection against drones, both at home and abroad.

Below is a description of key doctrine from across the Joint Force, which can help shape future study:

Joint Publication 3-01, *Countering Air and Missile Threats*. Defines counterair as integrating offensive and defensive operations to achieve air superiority and protect forces from aircraft and missile threats. It also frames integrated air and missile defense as a theater-level approach combining counterair, global strike, homeland defense, and other capabilities.

Joint Doctrine Note 1-26, *Fundamentals of Counter-Unmanned Aircraft Systems*. Designed to aid warfighters engaged in Operation Epic Fury, where Iranian drones such as the Shahed-136 imposed risks to mission and force. It incorporates emerging joint practice within Operation Epic Fury, emerging Service doctrine and lessons learned, Joint Interagency Task Force 401 materials, Security Assistance Group-Ukraine materials, and academic materials.

Joint Interagency Task Force 401, *C-sUAS Urban Defense Pocket Reference*. Provides a quick reference for tactical leaders to design fixed site protection against drones in the homeland.

Joint Interagency Task Force 401, *Counter-UAS Operations: Safe-*

guarding Freedoms & Preserving Privacy. Explains how to integrate multi-sensor detection into layered defense for homeland protection against drones while operating in accordance with federal law and communications regulations to ensure both public safety and privacy.

Joint Interagency Task Force 401, *Physical Protection of Critical Infrastructure: Reframing Critical Infrastructure Security for the Drone Threat.* Explains how to think about physical protection against drones in new ways that include solutions that are layered, outward-looking, and focused on denying access, visibility, and opportunity, well beyond the entry gate or perimeter. Importantly, many of these measures do not require specialized counter-drone systems.

Joint Interagency Task Force 401, *Counter-Small Unmanned Aircraft Systems (C-sUAS) Quick Reference Guide.* Provides an overview for addressing drones across the spectrum of counter-drone capabilities.

Army Techniques Publication 3-01.81, *Counter-Unmanned Aircraft System Operations.* Provides guidance for planning and executing counter-drone operations across all echelons of the U.S. Army. It integrates detection, identification, and defeat methods into tactical and operational planning to protect forces from unmanned aerial threats.

Air Force Doctrine Publication 3-01, *Counterair Operations.* Provides guidance for achieving air superiority across conflict types, including operations involving drones. It emphasizes that air superiority may be unattainable in peer conflict, requiring adaptive and flexible counterair measures.

Marine Corps Tactical Publication 3-01A, *Scouting and Patrolling—Reaction to an Enemy Unmanned Aircraft.* This tactical publication explains how patrols detect, respond to, and survive attacks from enemy drones. It highlights the reconnaissance, targeting, and attack roles adversary unmanned systems now provide at low cost and scale.

Marine Corps Reference Publication 3-20F.8, *Low Altitude Air De-*

***fense Battalion* Handbook.** This publication addresses a key component of the counter-drone fight from a U.S. Marine Corps perspective. It provides a tactical-level view that complements the higher-level joint doctrine.

Navy Tactics, Techniques, and Procedures 3-10.1, *Naval Coastal Warfare*. This document provides tactics, techniques, and procedures for detecting and responding to threats approaching littoral zones. Its principles are readily applied to countering drones in coastal and maritime operational contexts.

Space Force Doctrine Document 1, *The Space Force*. This capstone doctrine establishes the Space Force's core purpose, roles, and integration with the Joint Force to deliver military effects in the space domain. Space-enabled capabilities—such as surveillance, communications, and positioning—are foundational to homeland awareness and support joint counter-drone operations.

1st Special Forces Command (Airborne), *UxS Handbook*. This publication provides the doctrinal foundation to enable U.S. Army Special Forces to meet the threat of drones at the tactical level of war.

SMALL DRONES, BIG PROBLEMS:
A First Principles Approach to Countering-UAS

By the order of the Director, Joint Interagency Task Force (JIATF) 401:

MATTHEW S. ROSS
Brigadier General, United States Army
Director, JIATF 401

Corresponding Author:

PAUL A. LUSHENKO, PhD
Lieutenant Colonel, United States Army
Chief Strategist, JIATF 401

DISTRIBUTION: United States Department of War, United States Joint Force, United States federal agencies and departments, and United States state, local, tribal, and territorial authorities.

Intentionally Left Blank


JOINT INTERAGENCY TASK FORCE
401