SAMPLE

Drone Attack

The Rise of the Attack Drone, the Scramble to Stop It, and the World's Honest Answer

Aiman Sterling

Free sample: Introduction & Chapter 1

putrabooks.github.io

Contents

Introduction

Chapter 1: The Crossing — How the Flying Machine Became a Weapon

Chapter 2: The Offense Catalog — What an Attack Drone Is

Chapter 3: The Target List — What Gets Attacked

Chapter 4: The Defense Stack — How You Stop a Drone

Chapter 5: The Economics of Asymmetry — The Invoice That Broke Air Defense

Chapter 6: The Laboratory — Ukraine and the Adaptation Cycle

Chapter 7: The Naval Curriculum — The Red Sea and the Escort Problem

Chapter 8: The Civil Frontier — Airports, Prisons, Stadiums, and the Law

Chapter 10: The Verdict — Are We Prepared?

Afterword

This free sample contains the Introduction and Chapter 1. The complete book contains the full contents above.

Introduction

On a September morning in 2019, a swarm of low-flying drones and cruise missiles struck the heart of Saudi Arabia's oil industry — the Abqaiq processing plant and the Khurais field — and, in a single stroke, knocked roughly half of one of the world's largest oil producers' output offline. The strike's imagery became iconic: the punctured processing towers, seen from above, looking less like an explosion site than like a sheet of paper shot through with a hole punch. Global oil prices jumped by the largest one-day margin in history. The weapons that did it cost, by the most credible public estimates, a few tens of thousands of dollars each. The infrastructure they hit was worth, and insured for, billions.

That single event condensed the problem this book is about. Small, cheap, commercially-derived flying machines — or their slightly militarized cousins — can now reach and destroy or disable targets that states spend billions to protect. They can be launched from far away, from pickup trucks, from basements; they can fly low and slow enough to be nearly invisible to systems built for aircraft and missiles; and they can be built, in their simplest forms, from hobbyist components by anyone with a workbench and a wiring diagram. The defense against them — radars that can see a bird-sized object, jammers, lasers, interceptor drones, missile batteries — costs orders of magnitude more per engagement than the attack.

In the 2020s this arithmetic went from theoretical to measured in real wars: the Houthi campaign in the Red Sea forced the world's most expensive navies to fire million-dollar missiles at thousand-dollar drones, sometimes in salvos; Ukraine became the largest drone war and counter-drone laboratory in history; and incidents from Gatwick Airport to the Kremlin lawn brought the same question home to ordinary life: what happens when anyone can fly a bomb, a camera, or a threat anywhere — and is anyone actually ready for it?

This book is the story of the attack drone and the world's defense against it. It begins with how the flying machine crossed into weaponhood; catalogues the offense and its target list; walks the full defensive stack — detection, disruption, interception — and its brutal economics; and follows the laboratories where the answer is being forged, above all Ukraine. It examines the civil frontier, where drones have paralyzed airports, smuggled contraband into prisons, and attempted assassinations; the industry and legal machinery racing to catch up; and the threat's next forms — swarms, autonomy, and mass. The final chapter delivers the verdict the title asks for: whether the world is, in any honest sense, prepared.

The short answer, and the reason this book exists: no — but the long answer is more interesting. The attack drone rewrote the economics of offense, and the defense is being rebuilt, in real time, in the only way such rebuilds ever happen: under fire. What follows is the field guide to that rebuilding, written while its lessons are still arriving daily from the front, and while every reader's own airspace is quietly being re-armed against a threat that, a decade ago, hardly anyone in authority took seriously at all.

Chapter 1: The Crossing — How the Flying Machine Became a Weapon

The attack drone did not arrive one day. It crossed over, and the crossing took seventy years of drift, punctuated by moments nobody quite recognized as the moment.

Unmanned flight is older than most people assume: powered drones flew in both world wars, and the mid-century decades produced target drones, reconnaissance aircraft, and missile-like cruise weapons — the ancestors of everything in this book. What kept them from being "drones" in the modern sense was the absence of the enabling triad: cheap computing, satellite navigation, and wireless data links. A weapon needs to know where it is, decide what it is doing, and report back — and until the late twentieth century, those capacities cost more than aircraft.

The breakthrough era came in the 1990s-2000s, when the Predator's famous video feeds made the military drone a household object, and the technology's real revolution happened offstage, in the commercial sector. The smartphone industry miniaturized the sensors — accelerometers, cameras, GPS chips, processors — and the hobbyist industry, led by the Chinese manufacturer DJI, turned them into flying cameras that anyone could buy for the price of a television. By the mid-2010s, a consumer quadcopter could hover precisely, stream high-quality video, follow a person, and return home on command. Every component of weaponhood except the weapon was on the shelf, retail, at commodity prices. The crossing, at that point, was only a matter of intent — and intent, as it turned out, was not in short supply.

The modern drone era began with an irony its founders did not foresee: the states that pioneered the armed drone spent two decades demonstrating, from altitude, exactly what a drone can do — the surveillance, the strike, the reach — while assuming, by the logic of every weapon before it, that the capability would remain theirs. The Predator era's strikes (the targeted- killing campaigns of the 2000s-2010s) taught the world's militaries, militaries-in-waiting, and non-state actors a single curriculum: the aircraft that finds and kills cheaply, without risking a pilot, is the weapon that matters. The lesson's early students were adversaries (Hizbullah's drone fleet, the Islamic State's bombers, the Houthi arsenals); its graduates, by the 2020s, were everyone.

The crossing was thus not a leak of technology but a collapse of assumption: a capability demonstrated at $4 million a copy proved, within twenty years, replicable at $400 — and the monopoly ended not with a test flight but with a marketplace. Every chapter of this book is a downstream consequence of that

collapse, and the Predator's final irony is that the first serious drone-defense curriculum on earth is being written against the weapon it invented.

The commercial revolution deserves its own paragraph, because its scale explains everything downstream. The Chinese manufacturer DJI — by the mid-2010s the dominant global maker of consumer drones, holding by most market accounts the overwhelming majority share — achieved something no defense program ever had: it put millions of stable, GPS- guided, camera-equipped, autonomous-capable aircraft into the world's hands at consumer prices. The cascade followed the price curve: every price drop expanded the operator base; every expanded operator base matured the component ecosystem (motors, flight controllers, batteries, radios); every matured component became, to an engineer with hostile intent, a catalog.

The war- grade FPVs of the 2020s are assembled from that catalog — racing frames, hobbyist radios, commodity cameras — and the improvised arsenals of non- state actors are drawn from it more directly still. The defense ministries of the world spent the 2010s watching the consumer cascade with an unease they struggled to justify in budget testimony; Abqaiq, Gatwick, and the FPVs of Ukraine wrote the justification for them.

The intent announced itself piecemeal. Non-state actors mounted grenades on hobbyist quadcopters in Iraq and Syria by the mid-2010s — improvised, janky, but the pattern was set: commercial drone plus explosive, aimed from overhead. The Islamic State's drone program grew into a documented campaign of droppable munitions and, before its territorial defeat, into attack drones that coalition forces spent real resources countering — the first sustained conflict between hobbyist hardware and military countermeasures. In parallel, the first civilian alarms sounded: the Gatwick Airport shutdown of December 2018, in which drone sightings — real, hoaxed, or panicked — shut one of the world's busiest airports for parts of three days, disrupted well over a hundred thousand passengers, and demonstrated that a device purchasable at a mall could close the infrastructure of a major nation without carrying a weapon at all. The attack drone, in 2018, was already a weapon even when it was unarmed.

Then came the event that ended all ambiguity, described in this book's opening: the September 2019 strike on Saudi oil infrastructure, claimed by Yemen's Houthis and widely attributed by Western governments to Iran, which demonstrated the strategic attack — infrastructure-level damage, from standoff range, for pocket-change cost. Defense ministries worldwide wrote the same memo that season. Somewhere between the hobbyist grenades of Mosul and the burning towers of Abqaiq, the question had stopped being

whether the drone would become an attack weapon, and become: what do we do now?

The answer was accelerated by war. Russia's 2022 full-scale invasion of Ukraine began as a conventional, twentieth-century war — armor, artillery, missiles — and evolved, within a year, into the first full-spectrum drone war: cheap FPV (first-person-view) racing drones converted into precision anti-armor weapons; commercial quadcopters doing reconnaissance and grenade drops; loitering munitions hunting radars and guns; massed long- range strikes on cities and infrastructure; and, on the other side, the fastest and largest counter-drone mobilization in history. Ukraine's experience became this book's core case study — the war that industrialized both sides of the ledger — and Chapter 7 tells it at length. But first, the anatomy of the threat itself: what the attack drone actually is, and what it can actually do.

End of free sample. The full book is available at putrabooks.github.io