

DEFENDING YOUR AIRSPACE IN THE DRONE AGE: A STRATEGIC BLUEPRINT FOR COUNTER-UAS DEFENSE

Amir Lavi ParaZero Technologies Ltd.



An image taken from a video shows a Ukrainian drone striking Russian planes deep in Russia's territory, June 1, 2025 (Ukrainian Security Service photo via AP).

parazero.com | LinkedIn | YouTube | Facebook | X

PROLOGUE From Innovation To Danger: The Story of Drone Threats

Over the last two decades, drones have gone through a dramatic metamorphosis. Initially celebrated as the wonder of innovation and symbols of technological progress, they were embraced across civilian sectors—from aerial photography and agricultural monitoring to parcel delivery and entertainment. Consumer models were once considered an expensive toy and were confined to hobby shops and tech expos, seen as harmless tools of creativity or leisure.

Through the years, the very features that made drones attractive to innovators—relatively low cost, ease of use, modularity, and remote operation—have made them equally appealing to adversaries around the world. What began as a technological toy has rapidly become one of the most disruptive threats on the modern battlefield.

This shift began slowly and gained momentum during conflicts such as those in the Middle East, where non-state actors, such as ISIS and Yemeni Houthis, demonstrated the lethality of commercially available drones modified with rudimentary explosives. It has since escalated into a strategic arms race, as seen bluntly in the Russia-Ukraine and Israel-Hamas conflicts. In Ukraine, homemade FPV (First Person View) drones costing less than \$500 have been used to destroy armored vehicles and radar systems worth millions. Hamas' drones have been weaponized to penetrate urban environments, attack surveillance nodes, and spread chaos beyond the front lines.

The line between commercial drones and military assets has blurred. Today's drone threat no longer resides solely in the sky- it lurks in innovation labs, e-commerce warehouses, and enemy training grounds. Their transformation is a case study in asymmetric warfare: how emerging technologies, when unregulated and exploited, can bypass the traditional military superiority of even the largest, smartest, and most trained armies in the world.

The Ukrainian drone swarm attack on the Russian strategic bombers last Sunday (June 1st, 2025) was a tactical masterclass in ingenuity and boldness. This attack showed the world, yet again, the power and place of drones in modern warfare. It should also serve as a red flag for those who wish to defend themselves from hostile drone attacks, from small FPVs to large-scale UAVs.

In the following pages, we aim to explore the transformation and weaponization of drones in detail, examining the landscape of Counter-UAS solutions from long-range, kinetic solutions such as Anti-Air missiles (ie. Israeli Iron Dome or David's Sling system), to shortrange, *"soft-kill"* solutions that are safe to use in urban environments.

CHAPTER I How Drones Changed and Will Continue to Change Modern Warfare

Drones have fundamentally transformed the landscape of modern warfare, shifting the paradigm from traditional, state-centric conflicts to asymmetric engagements where non-state actors can wield significant power. The accessibility, affordability, and adaptability of unmanned aerial vehicles (UAVs) have enabled a diverse array of actors to wage aerial-based operations that threaten critical civilian infrastructure, governmental sites, armored convoys, and individuals across the battlefield.

Houthis: Strategic Strikes On Critical Infrastructure

The Houthi terror movement in Yemen has pioneered the use of low-cost drone warfare as a strategic tool to threaten regional powerhouses. Their drone campaign against Saudi Arabia is one of the most sustained and tactically sophisticated uses of UAVs by a non-state actor in modern conflict.

One of the most prominent examples occurred on **March 7, 2021**, when the Houthis launched a coordinated barrage of **14 drones** aimed at key Saudi energy and military assets. The primary target was **Ras Tanura**, one of the largest oil shipping ports in the world, operated by **Saudi Aramco**. Additional strikes were aimed at **military facilities in Dammam, Asir, and Jazan**, indicating a layered attack strategy designed to stretch air defense resources and overwhelm response systems.



Saudi Aramco Fuel Depot Hit by Houthi Drone Attack Source: <u>Bloomberg</u>

The Houthis used a mix of drones, including the **Qasef-2K**, a kamikaze drone modeled on the Iranian Ababil-T, often modified to carry high-explosive warheads. By targeting Ras Tanura, the Houthis attempted to strike not just a military blow but an economic one, threatening **5% of the world's daily oil supply** and demonstrating that even strategic national infrastructure was within reach of asymmetric actors.

While Saudi air defenses managed to prevent a catastrophic hit, the incident was a clear signal: non-state actors, with foreign backing and commercial drone adaptation, can now challenge sovereign airspace and economic stability at a strategic level.

This was not an isolated event. From 2019 to 2023, the Houthis have conducted **dozens of drone strikes** targeting Saudi airports, refineries, desalination plants, and even the capital Riyadh. These attacks show a pattern of escalation and growing technical sophistication, including the use of long-range UAVs capable of flying over **1,000 km**, evading radar through low-altitude flight profiles, and hitting precision targets with lethal efficiency.

The implications are profound. The Houthi campaign highlights a **new paradigm in hybrid warfare** where drones are not just tools of harassment—they are weapons of economic disruption and psychological intimidation. By exploiting the inherent weaknesses in conventional air defense networks— designed for large, fast-moving targets rather than swarms of slow, low-flying drones— the Houthis and their supporters have redefined the cost-benefit calculus of strategic deterrence.



Saudi Aramco Fuel Depot Hit by Houthi Drone Attack Source: <u>The New York Times via Reuters</u>

Sources:

- 1. MEPEI- Middle East Political and Economic Institute
- 2. Reuters, March 7th, 2021
- 3. <u>The New York Times</u>
- 4. <u>Bloomburg</u>

Russia–Ukraine Conflict: The Rise of Tactical FPVs and Strategic Fiber-Optic Drones

The Russia–Ukraine War has become the most drone-intensive conflict in history, transforming how both kinetic and electronic warfare are fought. Drones are not simply supporting elements—they are now central to operations, both at the tactical level in trench warfare and in long-range strategic strikes. Ukraine, in particular, has emerged as a leader in low-cost, high-impact UAV innovation.

Frontline Dominance with FPV Drones

On the battlefield, **First Person View (FPV)** drones have become the weapon of choice for both sides. Built from commercial racing drone components, these drones cost as little as \$400–\$600 but routinely disable or destroy Russian vehicles, bunkers, and electronic warfare assets worth tens or hundreds of thousands of dollars, if not millions.

Ukrainian FPV drones are often manually piloted via onboard cameras, delivering explosive payloads directly into confined tank hatches or entrenched defensive positions, and chasing soldiers across the battlefield. This mode of operation allows for real-time tactical adjustments, making them highly accurate even in cramped environments such as trench lines or urban ruins.



Russia - Ukraine Conflict | FPV chasing a soldier

Recent estimates suggest that **over 60% of Russian frontline armor losses** are now attributed to FPV drones—a stunning testament to their effectiveness (<u>Bloomberg</u>). Ukraine's military-industrial ecosystem now produces **thousands to millions of these drones monthly**, supported by local 3D printing and civilian crowdfunding efforts.



Russia - Ukraine Conflict | FPV chasing soldiers

Strategic Strikes with Fiber-Optic Controlled Drones

At the strategic level, Ukraine has escalated the conflict by developing **long-range drones that use fiber-optic guidance systems**—a critical innovation in bypassing Russian electronic warfare (EW) defenses.

Traditional drones often rely on GPS or radio frequency (RF) links to maintain navigation and control, making them vulnerable to jamming and spoofing. To counter this, Ukraine has begun deploying drones equipped with **fiber-optic cables**, enabling them to remain connected to their operators even in contested radio frequency environments. This innovation renders GPS jamming and RF scrambling ineffective, opening a new dimension in low-signature, precision-guided, long-range drone warfare.



Ukrainian-made fiber optic drones are already operating at the front Source: Brave1

A dramatic example of this was seen during **Operation Spiderweb** on **June 1, 2025**, when Ukraine launched a series of deep-strike drone attacks against multiple Russian airbases. Over **40 military aircraft**, including Tu-95 and Tu-22M strategic bombers, were damaged or destroyed. The drones used in the attack were covertly inserted into Russian territory in mobile wooden units, then deployed using fiber-optic or autonomous inertial navigation to evade Russian air defenses (<u>AP News</u>).

These fiber-optic drones represent a **new frontier in airpower**—a battlefield innovation that blends commercial technology with military-grade tactical design to exploit the vulnerabilities of traditional C-UAS systems.

A Redefinition of Air Superiority

Russia, likewise, has deployed Iranian-designed Shahed drones in mass strikes on Ukrainian cities and infrastructure. But the tactical and strategic balance is increasingly shifting in Ukraine's favor due to their domestic drone innovation, battlefield agility, and adaptive command structures.

FPVs and fiber-optic drones have done more than disrupt the battlefield—they've redefined **air superiority** as something that can now be achieved from a trench, a barn, or a civilian workshop. This democratization of precision airstrike capabilities is one of the most defining features of 21st-century conflict.

Israel-Hamas: Drone-Led Assault Doctrine

During the raid of Hamas on the Kibbutzim (communities) surrounding the Gaza Strip on October 7th, 2023, Hamas' use of drones had a significant impact on the Israeli Defense Force (IDF) defensive arrays across the border.

Within the first 30 minutes of the attack, small, off-the-shelf drones outfitted with a grenade or a mortar shell and a \$19.99 release-and-drop mechanism purchased via AliExpress, were used to neutralize and destroy the IDF's frontal observation cameras, communication towers, and remote-controlled heavy machine guns mounted on outposts designed to prevent these types of invasion. This attack was a strategic blow as it almost instantly neutralized the IDF's ability to detect, communicate, and remotely respond to the raid.



Hamas Attack on October 7th, Remote-controlled Machine Gun Outpost Source: <u>Ynet</u>

The same technique was used to neutralize small groups of infantry soldiers and a few of the IDF's "*Merkava"* main battle tanks. The Markava Tank Mark 4B is one of the few tanks in the world that is equipped with an active defense system against projectiles, Rafael's "*Trophy*" system; however, at the time, it was not capable of dealing with such threats.







Hamas Attack on October 7th, Nachal Oz Base Source: <u>"The Battle on Nachl Oz" Kan 11 - Israeli Broadcasting</u>

Hamas' ability to conduct tactical sabotage in key elements of the battlefield, such as cameras and communication, by exploiting drones' versatility and the element of surprise, turns urban alleys and heavily armored outposts into a potential "kill zone". This forces ground troops and commanders to account for an entirely new vertical dimension in both defensive and offensive operations.

Warfare is Now 3D and Distributed

Modern warfare has expanded from the two-dimensional battlefield of ground and armor to a fully three-dimensional operational space. This is not a future scenario- it is now a doctrine. Drones are fast, small, nearly silent, and multi-directional. They scale unpredictably—from a single FPV suicide drone to a 100-unit swarm—and adapt instantly to target vulnerabilities. Importantly, they challenge the value proposition of legacy systems: a \$500 drone can now defeat radars, missile systems or critical infrastructure that can cost millions.

CHAPTER II Counter-UAS Solutions: The Good, The Bad and the Ugly

The current counter-drone ecosystem includes a range of both soft-kill (non-destructive) and hard-kill (kinetic) solutions, each suited to different threat environments, operational constraints, and technological assumptions. To evaluate their effectiveness, we compare them across four critical parameters: **cost**, **range**, **urban safety & collateral damage**, and **deployability at scale**. Cost reflects acquisition, integration, and maintenance expenses.

Range determines the system's effective engagement envelope—whether at close proximity or over long distances. Urban safety and collateral damage weigh the risk each system poses to civilians and infrastructure, especially in populated environments. Finally, deployability at scale refers to how easily a solution can be mass-produced, transported, and operated across a distributed battlefield.

This matrix reveals that while traditional hard-kill systems like MANPADS (Man-Portable Air Defense System) and kinetic interceptors provide definitive effects, they are often expensive, risk collateral damage, and are logistically difficult to scale. On the other hand, soft-kill systems like RF jamming and protocol hijacking are cost-effective and safe in civilian zones, but can struggle against autonomous drones or those hardened against EW interference..



Soft-kill Solutions

RF Jamming

RF jamming is a technique that disrupts the communication link between a drone and its operator by emitting signals on the same frequencies, causing the drone to lose control or enter a fail-safe mode. It is widely used by troops and law enforcement personnel to safeguard events with big crowds, VIPs, and/or sensitive facilities. For instance, during Pope Francis' funeral in April 2025, Italian forces deployed small RF anti-drone gun squads around St. Peter's and Saint Martha House, ready to take down any unauthorized drone entering the premises and disrupting the funeral. (Euro News)



RF Squads in the Street of The Vatican Source: <u>Euro News</u>

Pros:

- Non-destructive method
- Effective against drones relying on radio control
- Immediate neutralization upon activation

Cons:

- Ineffective against autonomous drones without active communication links
- Potential to interfere with other critical communications in the vicinity
- Regulatory restrictions in certain jurisdictions

Cost: Relatively low Range: Short to Mid Collateral Damage: Medium (risk of unintended signal disruption) Urban Safety: High Deployability at Scale: High - easy to adopt

GPS Spoofing

GPS spoofing is a technique that misleads a drone's navigation system by broadcasting counterfeit satellite signals, causing the drone to miscalculate its position. This can lead the drone to drift off course, return to a false home position, or land in a controlled area. The method is gaining popularity among both military and critical infrastructure operators for its stealth and non-destructive profile.

A prominent example comes from the Syrian conflict, where Russian forces reportedly used GPS spoofing to protect the Khmeimim Air Base from U.S. and Israeli surveillance drones. Researchers from the University of Texas, collaborating with the Center for Advanced Defense Studies (C4ADS), detected GNSS spoofing originating from the Khmeimim Air Base on three separate occasions. These spoofing activities were aimed at misleading drones and aircraft, effectively neutralizing multiple incursions without physical engagement. ("*Above Us Only Stars*" report by University of Texas and C4ADS)

Pros:

- Non-kinetic and invisible to human observers
- Can redirect or capture drones without physical damage
- No physical damage to the surroundings

Cons:

- Limited effectiveness against drones using protected inertial navigation or preprogrammed routes
- Requires precise timing and strong signal power
- GPS disruption to friendly or civilian systems

Cost: Medium

Range: Wide

Collateral Damage: Medium collateral effect on everyone within the broadcasting range, from smartphones to civil aviation.

Urban Safety: High

Deployability at Scale: Medium

Cyber Takeover

Cyber Takeover is a sophisticated counter-drone technique that involves intercepting and assuming control over unauthorized drones by exploiting vulnerabilities in their communication protocols. Unlike jamming or GPS spoofing, cyber takeover allows operators to safely commandeer rogue drones, redirect them, or land them in designated areas without causing physical damage.

A notable real-world application of this technology occurred during Pope Francis' visit to Slovakia in 2021. The Slovakian Ministry of Interior employed <u>D-Fend Solutions' EnforceAir</u> <u>system</u> to protect the Pope and attendees from potential drone threats during multiple events. During an open-air Holy Mass in Šaštín attended by approximately 60,000 worshippers, a suspicious drone was detected. Instead of using jamming techniques, which could have disrupted communications, authorities utilized EnforceAir to take control of the drone and safely land it away from the crowd, ensuring the event proceeded without incident (<u>DroneLife</u>).

Pros:

- Non-kinetic and non-destructive method
- Allows for safe redirection or landing of drones
- High precision; ideal for use near crowds or critical infrastructure
- Enables data capture from hostile drones (forensics)

Cons:

- Irrelevant against fiber-optic, encrypted or completely autonomous drones
- Requires access to specific drone communication protocols
- Subject to state or regional regulations and restrictions

Cost: Intermediate Range: Short to Mid Collateral Damage: Low Urban Safety: Very High Deployability at Scale: Medium – scalable via mobile units and stationary posts

Hard-Kill Solutions

Kinetic Interceptors - Iron Dome

Iron Dome is an Israeli mobile all-weather air defense system developed by Rafael Advanced Defense Systems and Israel Aerospace Industries. Originally designed to intercept and destroy short-range rockets and artillery shells, the system has evolved to counter a variety of aerial threats, including unmanned aerial vehicles (UAVs). Its versatility allows it to protect both civilian populations and critical infrastructure.

A notable instance of Iron Dome's capability occurred in May 2021, when it successfully intercepted a UAV launched from the Gaza Strip. This marked the first time the system was used operationally to down a drone during combat, demonstrating its adaptability to emerging threats (<u>Times of Israel</u>). Since its first drone interception in May 2021, the Iron Dome has been able to intercept many of the hostile drones launched by Hamas from the Gaza Strip and Hezbollah from Lebanon.



Iron Dome Interception of multiple drones Source: Israeli Ministry of Defense YouTube Channel

Pros:

- Proven effectiveness and high success rate (over 90%) against a range of aerial threats, including rockets and drones
- Rapid response time with real-time threat assessment
- Mobile deployment enables flexible positioning in response to changing threat dynamics

Cons:

- High operational costs per interception
- Potential saturation during mass attack scenarios
- Limited effectiveness against very low-flying or small UAVs without system enhancements

Cost: High

Range: Short to Mid

Collateral Damage: High

Urban Safety: Low due to interception fragments

Deployability at Scale: Medium to Low– requires significant infrastructure, investment and training

Directed Energy Weapons (DEWs)*

Directed Energy Weapons (DEWs) utilize concentrated energy, such as lasers or microwaves, to neutralize aerial threats by damaging or destroying their critical components. These systems offer rapid response times and can engage multiple targets with minimal operational costs, making them increasingly vital in modern air defense strategies.

In May 2025, Israel became the first country to successfully deploy high-powered laser weapons in active combat, intercepting and destroying enemy drones. The Israeli Air Force's Aerial Defense Array operated a prototype high-power laser system developed by Rafael Advanced Defense Systems.

This system, a precursor to the larger Iron Beam project, was used to down drones launched by Hezbollah along the Lebanese border. The Israeli Ministry of Defense released footage showing the laser system igniting drones mid-air, leading to their destruction. This milestone demonstrates the practical application of laser-based defense systems in realworld combat scenarios. (Business Insider)



Laser Weapon Intercepts Enemy Drone Source: Israeli Ministry of Defense YouTube Channel

Pros:

- Extremely low cost per interception (estimated at a few dollars)
- Unlimited "magazine" capacity, allowing for continuous operation
- Silent and precise

Cons:

- Effectiveness can be reduced by adverse weather conditions like rain, fog, or dust
- Requires significant power supply and cooling systems
- Currently have proven effectivness against slower-moving or stationary targets

Cost: Low per interception; high initial setup cost Range: Short to Mid (up to 10 km) Collateral Damage: Low–precision targeting minimizes unintended damage Urban Safety: High–silent operation and precision reduce risks in populated areas Deployability at Scale: Low – high investment in infrastructure

*DEW technology is relatively new in terms of operational capabilities and analysis; more data is required to make a mindful assessment.

No Silver Bullet

The spectrum of counter-UAS technologies is broad, innovative, and rapidly evolving—but it remains far from perfect. While this chapter focused on several leading systems and techniques, it is by no means exhaustive. Emerging tools like high-powered microwave weapons, drone-on-drone swarms, and advanced radar-EO fusion platforms are also shaping the future of drone defense, each with its own trade-offs and operational niche.

Yet the central truth persists: **there is no such thing as a perfect system**. No single solution offers 100% coverage, foolproof interception, or universal applicability. Even the most sophisticated platforms—like Iron Dome or cyber takeover tools—have operational gaps, cost barriers, or limitations in certain environments. There is no "one to rule them all" in the world of drone defense.

As threats diversify and adversaries adapt, the counter-UAS challenge demands layered, context-driven, and adaptive architectures. Understanding the capabilities and limits of each tool is not just technical—it's strategic. Only by integrating these systems thoughtfully can security forces hope to regain airspace dominance in the age of ubiquitous drones.

CHAPTER III Multi-Layered Counter-UAS Defense Array: The Smart Solution

The modern drone threat is not a monolith. It is fast, layered, and distributed—and so must be the response. No matter how advanced, no single sensor, weapon, or system can provide full-spectrum protection against the diverse and evolving capabilities of modern UAVs. The concept of **layered defense**, long a pillar in traditional missile defense, is now indispensable in the world of counter-UAS (C-UAS).

This necessity becomes especially urgent in **urban and low-altitude environments**, where drones often operate under radar, behind buildings, or within civilian airspace. Here, the window for interception narrows from kilometers to meters, and the decision loop shrinks to seconds. At these ranges, **last-mile defenses** are not just a redundancy—they are the final layer between a threat and a catastrophic breach.

The Case for a Multi-Layered C-UAS Architecture

A robust C-UAS defense is built on three functional layers:

- 1. **Long-range detection and interception** (e.g., radar arrays, long-range missiles, or wide-area jamming).
- 2. Mid-tier engagement systems (RF disruption, spoofing, protocol takeover).
- 3. Last-mile neutralization—the point of no return.

Most current strategies emphasize the top two tiers, leaving a dangerous blind spot at the point of impact, particularly in **crowded urban areas**, military base perimeters, or near soft targets such as critical infrastructure, stadiums, or government compounds.

Autonomous FPVs and manually piloted micro-drones are increasingly designed to evade or absorb higher-tier defenses, slipping past jammers or avoiding radar through terrain masking and speed. Once inside the final few hundreds meters, **the tactical need shifts from detection to precision interception**, with safety, legality, and speed as top priorities.

Urban Battlespace, Civilian Rules

The tactical landscape is shifting from open fields to **city streets and industrial zones**. On 19 October 2024, a drone strike launched by Hezbollah from Lebanon detonated against the bedroom window of Israeli Prime Minister Benjamin Netanyahu's private residence. The operators were able to evade Israel's robust array of Iron Dome AA batteries and GPS interference among other countermasures, and navigate their way to the densely populated residential neighborhood in the town of Caesarea. The building did not suffer from substantial damage thanks to the materials chosen for the windows in the PM's house. (YNET, Israeli News).



Israeli PM's Private residences after a Hezbollah suicide drone attack In these environments, kinetic solutions such as missiles or directed energy weapons may pose unacceptable risks to civilian infrastructure, friendly forces, or even the defending operator. The engagement envelope becomes a high-stakes problem of **safe interdiction** in confined airspace.

Precision at the Edge

It is here that the final layer of defense must operate—with speed, accuracy, and safety. Whether handheld, drone-mounted, or static, the tools used to intercept hostile drones at close range must be highly discriminating, minimizing collateral impact while delivering certainty of the interception effect. These systems are not replacements for long-range C-UAS—they are its necessary complement in the event of a defensive breach such as the Israeli PM's house incident as described above.

Systems at the Tactical Edge

A growing class of solutions is emerging to fill this gap—systems purpose-built for **last-mile encounters**. These tools vary in form but share key characteristics: <u>low cost, rapid scalability, strong urban safety profiles, minimal collateral effects, and immediate response</u> capability.

Among them, modular platforms like **ParaZero's DefendAir** are gaining traction for their adaptability and operational flexibility. This net-based solution is offered in **three operational configurations**:

A **handheld personal net gun**, designed for soldiers or law enforcement officers to neutralize incoming threats at close range before impact.



DefendAir Personal Net Gun In Action Source: <u>ParaZero Technologies</u>

• An **autonomous drone interceptor**, capable of detecting, tracking, and executing high-speed mid-air interceptions using precision net deployment.



DefendAir FPV High-Speed Pursuit In Action Source: <u>ParaZero Technologies</u> • A stationary point-defense unit, mounted on or near government buildings, base perimeters, or critical infrastructure nodes and equipped with a detection system and autonomous net deployment mechanisms.



DefendAir Stationary Configuration (Ilustration) Source: <u>ParaZero Technologies</u>

Rather than replacing broader-layered systems, solutions like DefendAir are designed to anchor the **last line of defense**— ensuring that if detection or long-range interception fails, a reliable safeguard remains at the point of impact—capable of neutralizing threats while protecting civilians and preserving operational safety in urban environments.

CHAPTER IV From Disruption to Defense: Rethinking Airspace Security in the Drone Age

The threat posed by drones is no longer emerging—it is fully realized, active, and global. From the streets of Kyiv to the skies above Israel, from urban ambushes to long-range strategic strikes, drones have transformed the nature of modern warfare and internal security. They are cheap, fast, unpredictable, and increasingly lethal.

As written in the lines above, there is no single system that can provide full-spectrum protection against the growing diversity of drone threats. Each technology—whether RF jamming, GPS spoofing, cyber takeover, kinetic interceptors, or directed energy—has its strengths and limitations. Cost, range, safety, and scalability must all be weighed in a battlefield environment where the line between civilian and combat zone is increasingly blurred.

What is clear is this: effective drone defense requires a layered strategy. One that combines early detection, mid-range disruption, and most critically—reliable last-mile neutralization. It is not enough to detect a threat. It must be stopped—safely, precisely, and quickly—before it reaches its target.

Nowhere is this more urgent than in urban and critical infrastructure zones, where traditional C-UAS tools may be too blunt, too slow, or too risky to deploy. In these settings, modular, low-collateral solutions like net-based last-mile systems are not luxuries—they are necessities.

The future of airspace security is not defined by a single "silver bullet" system. It will be shaped by smart integration, adaptable deployment, and decisive last-line action. To defend the new battlespace, we must think in layers, plan for failure, and always protect the final meter.

Governments, defense organizations, and security agencies must act now. The speed at which drone threats are evolving leaves no room for reactive thinking. We urge stakeholders to:

- Audit and assess existing C-UAS capabilities across all tiers of engagement.
- Invest in modular, scalable last-mile solutions that can operate safely in urban and civilian-dense environments.
- **Integrate layered defenses** across detection, disruption, and interception—with fail-safes designed for the final few hundreds meters.
- **Prioritize field testing and interoperability**, ensuring technologies can be deployed under real operational conditions.

Airspace security is no longer a matter of dominance. It is a matter of survival. Let us defend forward—layered, precise, and uncompromising.