BIPSS Commentary
www.bipss.org.bd
May -2025
BIPSS Towards a Secure World

The Future of Airpower: Drones, Stealth and Swarming Tactics

Nabib Bin Zahid[1]

Source: Meshmerize[2]

Introduction

In an era defined by rapidly evolving threats and geopolitical uncertainty, the sky is no longer the limit—it's the next frontier of strategic dominance. From the relentless buzz of autonomous drones hovering at the edge of contested airspace to the whispered promise of near-invisible stealth platforms slipping through enemy defenses undetected, the Future of Airpower is being rewritten before our eyes. Swarming tactics—swarms of low-cost, networked unmanned aerial vehicles (UAVs) working in concert—threaten to upend traditional notions of deterrence and defense. Cybersecurity of these systems remains a critical vulnerability. As state and non-state actors alike embrace these cutting-edge capabilities, legal, ethical, and technical challenges multiply: How do we regulate autonomous targeting? Can existing international treaties keep pace with rapid innovation? And what are the implications for civilian safety and privacy? This commentary delves into the transformative potential of next-generation airpower, drawing on lessons from recent

[1] Nabib Bin Zahid is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). He has completed his B.S.S in International Relations from the University of Rajshahi.
[2] https://meshmerize.net/wp-content/uploads/2023/08/drone-big-1024x640.jpg

conflicts in Ukraine, the Middle East, and the Indo-Pacific. This commentary will examine how nations, industry leaders, and international institutions must adapt procurement strategies, embrace resilient architectures, and foster robust governance frameworks. Prepare to explore the decisive technologies that will determine air superiority in the coming decades—and to confront the hard choices inherent in wielding them responsibly.

Historical Evolution of Airpower

Early Unmanned Experiments

The foundational concept of unmanned aerial vehicles (UAVs) emerged during World War I. In March 1917, Britain tested the "Aerial Target," a small radio-controlled craft designed for gunnery practice. Shortly thereafter, in October 1918, Charles F. Kettering's "Kettering Bug" successfully flew as an experimental aerial torpedo capable of traveling some 75 miles at roughly 50 mph before its wings were jettisoned and it descended onto its target. Although neither system saw combat, these pioneering efforts demonstrated the feasibility of self-piloted machines and laid the groundwork for modern cruise missiles and reconnaissance drones[3].

Cold War Stealth Breakthroughs

Amid intensifying superpower rivalry, airpower evolved to emphasize survivability against advanced air defenses. Lockheed Martin's Skunk Works was instrumental, first with the U-2 high-altitude spy plane (1955) and then the Mach 3-capable SR-71 Blackbird (first flight 1964). However, the game-changer arrived in the mid-1970s with the classified Have Blue demonstrator, which validated faceted airframe geometry to scatter radar waves. This research directly led to the F-117 Nighthawk—first flight in 1981 and operational in 1983—the world's inaugural operational stealth attack aircraft, combining low observability with precision strike capability[4].

Modern Drone Milestones

The evolution from remotely piloted prototypes to armed UAVs accelerated in the late 20th century. Israeli-born engineer Abraham Karem's DARPA-backed "Amber" and subsequent "Gnat" prototypes evolved into the U.S. Predator program after General Atomics won a development contract in January 1994. The MQ-1 Predator achieved its first flight in July 1994, deployed overseas in 1995 for reconnaissance, and by 2001 carried AGM-114 Hellfire missiles for precision

[3] A brief history of drones | imperial war museums. Accessed June 15, 2025. https://www.iwm.org.uk/history/a-brief-history-of-drones.

[4] Team, SOFREP News. "The Dawn of Stealth: Unveiling the Lockheed Have Blue Project." SOFREP, July 22, 2023. https://sofrep.com/news/the-dawn-of-stealth-unveiling-the-lockheed-have-blue-project/.

strike missions. This marked the first integration of autonomous surveillance with lethal capability, inaugurating a new era of remotely delivered airpower[5].

The Rise of Autonomous Drones

Types & Capabilities

Modern autonomous drones range from small multi-rotor UAVs to fixed-wing and hybrid VTOL (vertical take-off and landing) platforms. Multi-rotors—such as quadcopters and hexacopters—excel in agility and low-altitude operations, ideal for reconnaissance and localized missions. Fixed-wing drones offer efficiency and longer endurance, making them suited for regional surveillance or communications relay. Hybrid VTOLs combine these strengths, providing take-off flexibility and extended flight endurance[6].

AI-Enabled Autonomy & Networked Architectures

The key advancement in today's airpower lies in AI-driven autonomy and networked coordination. Autonomous UAVs utilize real-time SLAM navigation, computer vision, and sensor fusion—such as LiDAR and photogrammetry—for collision avoidance and waypoint tracking. Communications architectures integrate ground control stations, ADS-B systems, and mesh-network links to support beyond-line-of-sight operations.

Networked capabilities—where multiple UAVs share telemetry and tasking—enable cooperative mission execution, analytical offloading to edge/cloud systems, and resilience through redundancy[7].

Cybersecurity & Vulnerabilities

Despite technical advances, autonomous drones expose critical cyber risks:

- Communication hijacking & spoofing: Attacks such as "Snoopy" and "Skyjet" exploit weak Wi-Fi links or compromised firmware to seize control[8].

---

[5] Smithsonian Institution. "General Atomics MQ-1L Predator A." Smithsonian Institution. Accessed June 18, 2025. https://www.si.edu/object/general-atomics-mq-1l-predator%3Anasm_A20040180000.
[6] Sihag, Vikas, Gaurav Choudhary, Pankaj Choudhary, and Nicola Dragoni. "Cyber4Drone: A Systematic Review of Cyber Security and Forensics in next-Generation Drones." MDPI, June 28, 2023. https://www.mdpi.com/2504-446X/7/7/430.
[7] Javaid, Shumaila, Nasir Saeed, Zakria Qadir, Hamza Fahim, Bin He, Houbing Song, and Muhammad Bilal. "Communication and Control in Collaborative Uavs: Recent Advances and Future Trends." arXiv.org, February 23, 2023. https://arxiv.org/abs/2302.12175.
[8] Sumaidaa, Sara, Hamda AlMenhali, Mohammed Alazzani, and Kyusuk Han. "Enhancing Security of Mobile Crowd Sensing in Unmanned Aerial Vehicle Ecosystems." Frontiers, June 19, 2025. https://www.frontiersin.org/journals/communications-and-networks/articles/10.3389/frcmn.2025.1443592/full.

- Malware injection and firmware manipulation: Attackers can introduce backdoors (e.g., "Maldrone"), corrupt flight code, or disrupt navigation systems.
- Flight-control software vulnerabilities: Autopilots like PX4 and Ardupilot contain hundreds of known bugs that may allow remote shutdown or erratic behavior[9].
- GNSS and ADS-B weaknesses: GPS spoofing and ADS-B manipulation threaten navigation and situational awareness.

Source: Military Aerospace[10]

Swarming Tactics: Redefining Force Multipliers

In the battlespace of tomorrow, it won't just be about bigger and faster—it'll be about *many*. Swarming tactics, where vast numbers of low-cost, interconnected drones flood the skies in coordinated assault, are rewriting the rules of airpower. Imagine dozens—if not hundreds—of autonomous UAVs acting as a single, intelligent organism, overwhelming even the most advanced defense systems. This is not science fiction; it's fast becoming military reality. In this section will unpack how drone swarms operate, why they're so effective, and what high-stakes trade-offs they bring to modern warfare's rapidly evolving playbook.

Swarm Theory & Doctrinal Origins

Swarming draws from natural behaviors found in insect hives, bird flocks, and fish schools, applied to military doctrine for coordinated, decentralized attacks. John Arquilla and David Ronfeldt's seminal 2000 RAND report defined swarming as a "coordinated, strategic way to strike from all

[9] Potential cyber threats, vulnerabilities, and protections of unmanned vehicles. https://cdnsciencepub.com/doi/full/10.1139/juvs-2021-0022.

[10] https://img.militaryaerospace.com/files/base/ebm/mae/image/2018/05/1804maeuv_swa.png?auto=format,compress&fit=max&q=45&w=950&width=950

directions, by means of a sustainable pulsing of force"[11]. In battlefield environments—especially where adversaries are stronger—swarms introduce surprise, agility, and mass in novel ways. Historically, even during the 1993 Mogadishu battle, swarming infantry overwhelmed U.S. forces with numbers and maneuver[12].

Cooperative Behaviors & AI Control

Modern swarms implement AI-driven algorithms to enable coordination without centralized control. Reinforcement learning models—such as Proximal Policy Optimization (PPO)—help drones collaborate in surveillance or attack phases, dynamically adjusting roles based on the mission[13]. Onboard edge computing and sensor-fusion protocols allow swarms to operate autonomously even under jamming or GPS denial. These systems enable real-time path planning, obstacle avoidance, and role adaptation during missions.

Case Studies: Lessons from Recent Conflicts

Ukraine's Use of Commercial Drones: Innovation at the Edge

On the battlefields of Ukraine, what began as improvised kits—think DJI quadcopters strapped with makeshift payloads and duct tape—quickly matured into combat-proven aerial systems[14]. One standout example is **Escadrone**, a volunteer-led Ukrainian group producing up to 1,000 FPV loitering munition drones monthly, each costing under $500, and designed to plunge into tanks and artillery. Similarly, Aerorozvidka's octocopter R18, deployed as early as 2019, has destroyed over 100 Russian vehicles by mid-2022, proving that even relatively simple platforms can punch hard when effectively employed.

[11] Kallenborn, Zachary. "A Plague on the Horizon: Concerns on the Proliferation of Drone Swarms." orfonline.org, October 22, 2024. https://www.orfonline.org/research/a-plague-on-the-horizon-concerns-on-the-proliferation-of-drone-swarms.

[12] "What You Need to Know about Drone Swarms." dronecenter.bard.edu, December 28, 2014. https://dronecenter.bard.edu/what-you-need-to-know-about-drone-swarms/.

[13] Crowley, Taylor. "Swarm Drones - the Future of Warfare Is Already Here." NSIN, March 7, 2025. https://www.nsin.us/swarm-drones/.

[14] Kullab, Samya, Thu Aug 08 10:19:18 EDT 2024, and Samya Kullab. "Ukraine Is Building an Advanced Army of Drones. for Now, Pilots Improvise with Duct Tape and Bombs." AP News, September 26, 2023. https://apnews.com/article/drones-ukraine-war-russia-innovation-technology-589f1fc0e0db007ea6d344b197207212.

Source: Council on Foreign Relations[15]

Perhaps Ukraine's most headline-grabbing drone operation came in early June 2025: **Operation "Spider's Web."** Over 117 FPV drones, coordinated via machine learning and local cellular networks, struck deep into Russian airbases—reportedly damaging strategic bombers protected by multi-layered defenses—and bypassed jamming by navigating through environmental cues rather than GPS[16]. This high-tech raid underscored how low-cost drones, backed by AI-enabled autonomy, can achieve disproportionate strategic impact—and delivered a humiliating psychological blow to adversaries.

Middle East: Iran-Backed Proxies and UAV Swarms

In the Middle East, Iran has systematically empowered proxies—Hezbollah, Hamas, Houthi fighters and Iraqi militias—with growing UAV capabilities. A notable escalation occurred in late 2023–2024, with over 180 drone and missile attacks targeting U.S. installations in Iraq and Syria. Many of these drones were launched in bursts—classic swarm tactics meant to saturate air defenses and test U.S. interception capabilities .

The launch of Shahed-type UAV swarms by proxies, often protected by Iran's advanced electronic support, highlights another key learning: swarms are not just tools of major powers, but also accessible asymmetric weapons for non-state actors . While many intercepted, their sheer volume pressured defense budgets and response strategies—and forced a growing dependence on point-defense systems and kinetic counter–UAV tools.

Ethical, Legal & Policy Implications

The rapid rise of autonomous drones and swarm tactics poses profound ethical dilemmas, legal uncertainties, and policy challenges. As these systems edge toward fully autonomous lethality,

[15] https://cdn.cfr.org/sites/default/files/styles/full_width_xl/public/image/2024/01/UkraineDrones_A_1.webp

[16] Law, Harry. "Ukraine Just Demonstrated What Agi War Could Look Like." Time, June 5, 2025. https://time.com/7291455/ukraine-demonstrated-agi-war/.

three interlinked domains demand urgent attention: meaningful human control, adherence to international law, and coherent export and proliferation safeguards.

Autonomous Lethal Targeting: Where Do We Draw the Line?

Autonomous weapon systems (AWS) are pushing boundaries. The **International Committee of the Red Cross (ICRC)** has made clear that meaningful human control must govern any AWS, ensuring that machines do not make irreversible decisions independently. Yet advancements such as Turkey's Kargu-2 drone underscore the legal and ethical tensions, as drones begin selecting and engaging targets without direct human intervention[17].

Source: *US Department of Defense / Sgt. Cory D. Payne, public domain*

Critics invoke the **Martens Clause**—the moral backbone of international humanitarian law (IHL)—and argue that delegating life-and-death decisions to machines is inherently abhorrent, undermining human dignity and accountability. Human Rights Watch warns that fully autonomous weapons violate the laws of distinction and proportionality by lacking human judgment in uncertain scenarios. In contrast, many military powers insist that existing IHL frameworks are sufficient, provided human operators retain oversight.

Ethics, Technology & Public Accountability

Public sentiment runs strong: polls consistently show that over half of citizens worldwide oppose delegating lethal decisions to machines. The **'Campaign to Stop Killer Robots'**, backed by NGOs and religious institutions, is pushing for preemptive bans and clearer governance. Meanwhile, the Vatican has urged a moratorium and the preservation of human judgment in all use-of-force decisions.

[17] Nasu, Hitoshi. "The Kargu-2 Autonomous Attack Drone: Legal & Ethical Dimensions." Lieber Institute West Point, September 6, 2024. https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical/.

On the tech frontier, solutions like **humanitarian algorithms** or "codified key safety switches" offer possible ways to embed IHL compliance in code, but their effectiveness remains unproven, and questions persist over real-time human oversight.

Conclusion: Charting the Skies Ahead – The Urgent Future of Airpower

As drones, stealth platforms, and swarming tactics redefine the contours of modern airpower, the global security landscape is entering uncharted territory. The convergence of artificial intelligence, autonomous weapon systems, and networked aerial operations is no longer a distant prospect—it is today's reality. From the urban battlefields of Ukraine to the contested waters of the Indo-Pacific, we are witnessing a paradigm shift in how air dominance is achieved and contested.

But with innovation comes responsibility. The rise of drone swarms and autonomous systems introduces not only unparalleled military advantages but also complex ethical, legal, and strategic dilemmas. Questions surrounding human control, proportionality in warfare, and the risk of miscalculation in machine-driven conflict are no longer theoretical—they demand answers now.

To secure the future of airpower, states must adopt forward-looking doctrines, invest in cyber-resilient architectures, and craft internationally binding regulations that uphold the principles of international humanitarian law. Public-private partnerships, arms control frameworks, and AI ethics must all converge to ensure that technological progress does not outpace moral and legal accountability.

The battlespace of tomorrow will be shaped not just by who has the most drones or the stealthiest jets, but by who can integrate them most intelligently, deploy them most ethically, and govern them most responsibly. As nations race to command the skies with next-generation capabilities, the real test lies not in their development—but in their discipline.

In the age of autonomous warfare, the air above us is more than a domain—it is a proving ground for global leadership, restraint, and innovation. The future of airpower is here. The question is: are we ready for it?