JULY 2026

RESEARCH PAPER

AI-ENABLED PURPLE TEAMING FOR COUNTER-DRONE SECURITY IN SAHEL

the case of fixed assets

RIDA LYAMMOURI

POLICY CENTER FOR THE NEW SOUTH

RP -11/26

AI-ENABLED PURPLE TEAMING FOR COUNTER-DRONE SECURITY IN SAHEL

the case of fixed assets

RIDA LYAMMOURI

TABLE OF CONTENTS

AI-ENABLED PURPLE TEAMING FOR COUNTER-DRONE SECURITY IN SAHEL: THE CASE OF FIXED ASSETS....2

Table of Contents....3

ACRONYMS....4

Executive Summary....6

Section 1: Introduction....10

Section 2: The Evolution of Drone Warfare in the Sahel Since 2023 and the Current Capabilities of JNIM, FLA, ISSP and ISWAP....11

Section 3: What Six Recent Attacks Reveal About the Threat to Fixed Sites....14

Section 4: The Time and Resources Armed Groups Invest in Building Drone Capability....17

Section 5: What Successful Attacks Tell Us About Defender Counter-Drone Capability....19

Section 6: Purple Team Simulation: Adversary Capability, Site Defenses, and the Cost-Loss Trade-off....23

- **6.1 Methodology and Framewrk....23**
- **6.2 Red Team — The Documented Attack Profile....26**
- **6.3 Blue Team — Current Site Defenses....28**
- **6.3.1 Attacks Blocked At Each Level of Counter-Drone Investment, Military Base, Current State....28**
- **6.3.2 Air Component as Drone-Plus-Ground Counter....29**
- **6.3.3 Conditions and Attack Patterns that Affect Defender Performance....29**
- **6.4 Purple Team — Response and Recommendations....30**
- **6.5 Expected Adversary Adaptation....31**

ACRONYMS

AB101 — Air Base 101 (Niamey)

AB401 — Air Base 401 (Tahoua)

ACLED — Armed Conflict Location & Event Data

CSIS — Center for Strategic and International Studies

CSP-DPA — Cadre Stratégique Permanent pour la Défense du Peuple de l'Azawad

CUAS — Counter-Unmanned Aerial Systems

DJI — Da-Jiang Innovations

EW — Electronic Warfare

FABF — Forces Armées Burkinabè

FAMa — Forces Armées Maliennes

FAN — Forces Armées Nigériennes

FDG410 — FlyDragon FDG410

FDS — Forces de Défense et de Sécurité

FLA — Front de Libération de l'Azawad

FOB — Forward Operating Base

FPV — First-Person View

GCS — Ground Control Station

GUR — Holovne Upravlinnia Rozvidky (Ukrainian Main Directorate of Intelligence)

HEAT — High-Explosive Anti-Tank

HPM — High-Powered Microwave

IED — Improvised Explosive Device

INSS — Institute for National Security Studies

IS — Islamic State

ISR — Intelligence, Surveillance, and Reconnaissance

ISSP — Islamic State Sahel Province

ISWAP — Islamic State West Africa Province

JNIM — Jama'at Nusrat al-Islam wal-Muslimin

KIA — Killed in Action

LGA — Local Government Area

MINUSMA — Mission Multidimensionnelle Intégrée des Nations Unies pour la Stabilisation au Mali

MNJTF — Multinational Joint Task Force

OSINT — Open-Source Intelligence

PCNS — Policy Center for the New South

PG-7V / PG-7V(M) — Protivotankovaya Granata-7V (RPG-7 HEAT warhead family)

RF — Radio Frequency

RPG — Rocket-Propelled Grenade

SAM — Surface-to-Air Missile

SBU — Sluzhba Bezpeky Ukrayiny (Security Service of Ukraine)

TB2 — Bayraktar TB2

TOR-M2K — Russian short-range surface-to-air missile system

UAS — Unmanned Aerial Systems

UCAV — Unmanned Combat Aerial Vehicle

VDP — Volontaires pour la Défense de la Patrie

VTOL — Vertical Take-Off and Landing

VEO — Violent Extremist Organization

POLICY CENTER FOR THE NEW SOUTH

Armed-group drone use in the Sahel and Lake Chad Basin has scaled from rudimentary commercial-quadcopter Improvised Explosive Device (IED) drops in 2023 to a capability set that now includes First-Person View (FPV) strikes with shaped-charge anti-armor warheads, fiber-optic FPVs that defeat radio-frequency jamming, coordinated drone-and-ground assaults on hardened airfields, and a 25-drone non-state swarm. Four groups—Jama'at Nusrat al-Islam wal-Muslimin (JNIM), the Azawad Liberation Front (FLA), Islamic State West Africa Province (ISWAP), and Islamic State Sahel Province (ISSP)—now operate armed drones across Mali, Burkina Faso, Niger, and Nigeria, with the FLA's capabilities placing it among the most advanced non-state actors using drones globally.

RIDA LYAMMOURI

Drawing on 245 documented strikes in the region and publicly available Ukrainian training data, our analysis found the following:

- The capability demonstrated in a strike reflects months to years of preparation, and the next capability is typically already in development before the current one is publicly used. This suggests that defenders sizing investment against the current strike record are preparing for a threat picture that is already eighteen months out of date.
- JNIM conducts the most drone strikes in the region but has stopped advancing, with no new capability demonstrated in over a year and its attacks increasingly prioritizing IED drops. Unlike kamikaze strikes, which by default destroys the drone on impact, a drone dropping IEDs can return and be used again. This allows JNIM to maintain the region's highest tempo while preserving its inventory.
- While the FLA conducts fewer strikes, they are increasingly ISR-supported and precise. In attacks, FLA released footage shows operators adjusting the lock after a first hit to strike a target again as it moves for cover, a demanding combination that demonstrates significant operator skill.
- Based on our modeling, we assess it is likely inventory, not capability, that currently holds these groups back from more damaging attack
- Defender counter-drone capability has been functionally absent across three years and 245 documented strikes. Counter-Unmanned Aerial Systems (CUAS) engagement appears in only ten cases, and high-investment military sites were all penetrated without any CUAS engagement.

The brief runs an AI-enabled purple-team simulation against this threat across military bases, mines, pipelines, and urban sites, testing four counter-drone investment tiers: no dedicated capability (Tier 0), soldier-carried systems (Tier 1), integrated defense systems (Tier 2), and a full-spectrum stack adding high-powered microwave and laser capabilities (Tier 3). The simulation finds that Tier 2 is the most effective procurement level, reducing expected losses by 48 to 89 percent across all four asset classes. Across the key findings that emerge from the simulation, three overarching conclusions stand out:

1. When and how an attack occurs changes how well the equipment defending the site performs.

Cheaper defensive setups tend to fail under the conditions and tactics that appear most frequently in the regional record.

The single largest source of uncertainty in what a site should expect to lose is how often it will be attacked, a figure most sites appear to estimate poorly. Misjudging local attack rates undermines investment alignment in CUAS.

At an equipped site, expected losses are moderated mostly on how many fighters arrive in combined drone-and-ground assaults, as counter-drone equipment does not engage the ground force - it does not replace conventional perimeter defense against ground assault, and the two should be planned together.

Attacks concentrate in the hot dry season. Thirty-two percent of documented attacks fall between April and June, against 23 percent across the four rainy-season months. This suggests readiness raised ahead of the April window prevents the most harm at any equipment tier.

Harmattan degrades a defense the most where sites are least equipped. Dust removes up to sixty percent of a lower tier's CUAS power in the simulation, yet raises casualties only about six percent, as those tiers stop few attacks in any conditions.

The adversary is already adapting around the counter-drone equipment defenders can procure

The simulation shows how often a site at the integrated-defense tier stops the incoming drone. A fiber-optic drone emits no radio signal to jam or detect, and the FLA has possessed the capability since July 2025.

The FLA flew 25 drones at Gao in March 2026. The swarm's modeled share of casualties grows only modestly over the next year, but the one documented swarm already carried four times the interceptors an integrated-defense site keeps ready.

The bars show the documented share of attacks flown by advanced operators, with our twelve-month projection. Skilled pilots evade more of the defense and strike the wounded again more often.

2. The adversary is already adapting around the counter-drone equipment defenders can procure.

Without upgrades to that equipment, defender performance against these groups will only worsen over time.

- The integrated-defense tier (Tier 2) stops standard drones about ninety percent of the time but fiber-optic drones only 51 percent, as a fiber-optic drone emits no radio signal for jamming or radio-frequency detection to act on. The FLA has held fiber-optic capability since July 2025, and the adversary gains most by shifting attacks toward this drone type.
- A integrated-defense site keeps about six interceptor rounds ready, which the 25-drone swarm the FLA flew at Gao exceeds several times over. Only one attack of this nature has been documented, and the modeled growth in the swarm's casualty share over the next year is modest, so the exposure is the interceptor count itself.
- The documented operator-skill mix shifted sharply, from about seventy-one percent basic operators in 2024 to 43 percent in 2025, and the projection puts one attack in four in advanced hands. More skilled pilots evade more of the defense and cause more casualties when they strike, and they fly the follow-up strike on the wounded more often.

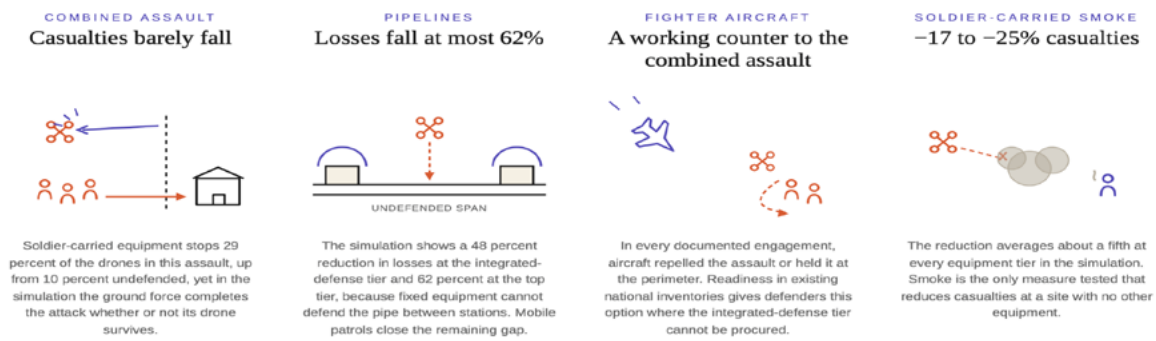
When and how an attack occurs drives the outcome as much as the equipment defending the site

3. Counter-drone equipment alone does not close the threat for some site profiles and attack modes.

Pairing that equipment with rapid-response aircraft and mobile patrols is as important as which tier the site procures.

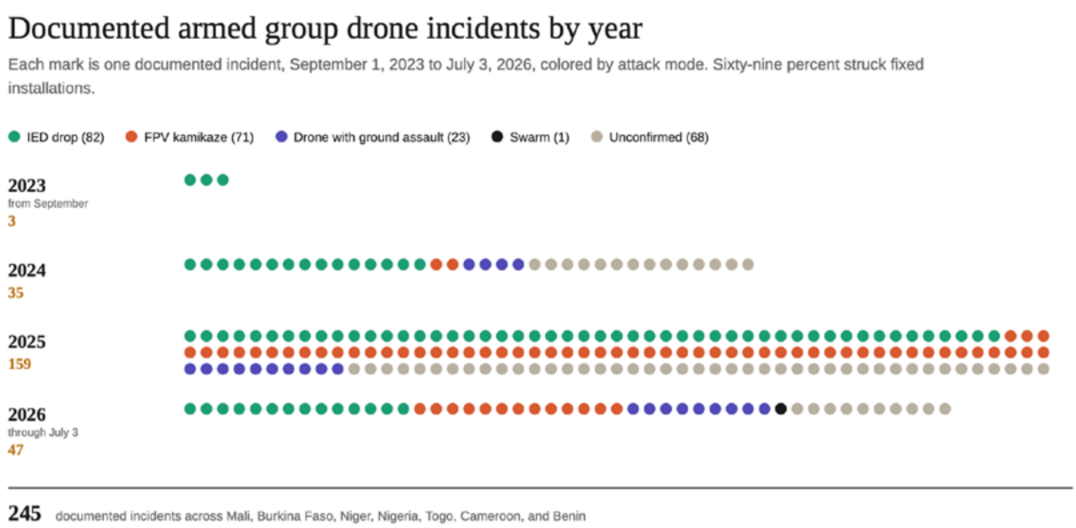
- Soldier-carried equipment (Tier 1) cannot stop the ground element of a combined drone-and-ground assault. It stops twenty-nine percent of the drones in that assault, up from 10 percent undefended, but casualties barely fall, as the ground force completes the attack whether or not its drone survives.
- Pipeline protection reaches a structural ceiling, cutting operational losses about forty-eight percent at the integrated-defense tier and 62 percent at the full-spectrum stack. Fixed equipment installed at pump stations and terminals cannot defend the pipe between them, and closing the gap further requires mobile patrols along the route.
- Rapid-response fighter aircraft are a documented counter to the combined assault. Where the integrated-defense tier cannot be procured, maintained air-component readiness gives defenders a working option against the worst-outcome attack mode in the regional record.
- Issuing soldier-carried smoke grenades and training troops to deploy them cut expected casualties by seventeen to 25 percent in the simulation, at every equipment tier and under both threat levels. It is the only measure tested that reduces casualties at a site with no other equipment, a soldier already wounded by the first strike can still deploy it against the follow-up strike, and it costs a small fraction of any equipment tier.

Counter-drone equipment alone does not close the threat for some site profiles and attack modes



SECTION 1: INTRODUCTION

Armed-group drone use in the Sahel and Lake Chad Basin has scaled rapidly over the past three years, moving from rudimentary commercial-quadcopter IED drops in 2023 to a capability set that now places the FLA among the most advanced non-state actors using drone operators globally. Capabilities demonstrated in the region include FPV strikes with shaped-charge anti-armor warheads, reported fiber-optic FPVs that can defeat radio-frequency jamming, coordinated drone-and-ground assaults on hardened airfields, and a non-state drone swarm. Acquiring any of these skills requires engaged operator training, sufficient drone stockpiles to absorb attrition through training, and expert team structures to provide critical support functions (explosive capabilities, ISR, etc). As the rate of knowledge diffusion increases, the lag between one group's adoption of the same capabilities has narrowed to as little as two months.



For this brief, we analyzed 245 armed-group drone incidents across Mali, Burkina Faso, Niger, Nigeria, Togo, Cameroon, and Benin between September 1 2023 and July 3 2026. Sixty-nine percent of these incidents struck fixed installations, including bases, forward operating positions, militia camps, gendarmeries, and unit positions. The gaps observed at these sites—no counter-drone systems or only basic ones, no perimeter surveillance, and no state-operated drones at forward posts—extend to the wider set of fixed assets that sit within armed groups' existing area of operations: artisanal and industrial gold mines, fuel import and distribution infrastructure, pipeline corridors, and ports. After discussing key milestones in armed group drone capability and current CUAS challenges over the past three years, this brief presents the results of an AI purple team simulation. The simulation uses the documented drone incidents, as well as Ukrainian primary-source training data, adjusted for Sahelian operating conditions, to model how counter-drone posture choices change expected losses at military bases, mines, pipelines, and urban targets. It then assess the strategic value and limitations of each posture, and how armed groups are likely to adapt to them. While this brief addresses the narrower question of how defensive choices change expected losses at fixed sites in the current conflict, it is important to remember that the conflict is ultimately driven by governance failures, local grievances, and contested state authority which fall outside of this scope.

SECTION 2: THE EVOLUTION OF DRONE WARFARE IN THE SAHEL SINCE 2023 AND THE CURRENT CAPABILITIES OF JNIM, FLA, ISSP AND ISWAP

Armed-group drone use in the Sahel and Lake Chad Basin has scaled rapidly over the past three years. In September 2023, JNIM conducted the first documented armed-group drone strike in the region, dropping IEDs on a Dogon militia camp in central Mali. By January 2026, ISSP was conducting a coordinated drone-and-ground assault on the Nigerien Air Force's primary military airfield in Niamey, and in April 2026 the FLA and JNIM seized parts of Kidal in northern Mali in a joint multi-axis assault that included FPV drone strikes on the city's Bayraktar TB2 ground control station and surrounding Malian and Russian Africa Corps positions.

Through mid-2025, the bulk of this activity was conducted by JNIM[1]. The group's drone activity expanded across Mali and into Burkina Faso, beginning with IED drops on a Burkinabé military detachment at Sollé in January 2024. By February 2025, the group was operating FPV platforms carrying plastic-bottle improvised explosive devices over Djibo, and by April 2025 they conducted their first kamikaze drone strike against the Togolese military outpost at Djignandjoaga – also their first drone strike in a third country.[2] Only one month later in May 2025, they kamikaze strikes against FAMa positions in Dioura, and by June, the group was conducting sustained drone operations across several national borders – the widest cross-border drone footprint of any armed group in the region. Since then, while the group has maintained a steady tempo of strikes, their capability development has not progressed significantly, with subsequent activity dominated by IED drops as opposed to new capability tiers.

The FLA began conducting drone strikes roughly ten months after JNIM. Its predecessor coalition, the CSP-DPA, conducted the first documented Tuareg-rebel drone strike during the Tinzaouaten battle in July 2024.[3] The FLA then progressed through capability tiers faster than JNIM had. In February 2025, it employed a Chinese-manufactured FlyDragon FDG410 (FDG410) Vertical Take-off and Landing (VTOL) surveillance drone, modified for strike use, against Tessalit airport.[4] The FDG410 has a payload capacity of up to ten kilograms, substantially above that of the commercial quadcopters used elsewhere in the region. In June 2025, the FLA conducted the first FPV strike with a Protivotankovaya Granata-7V (PG-7V) high-explosive anti-tank shaped-charge warhead against an Africa

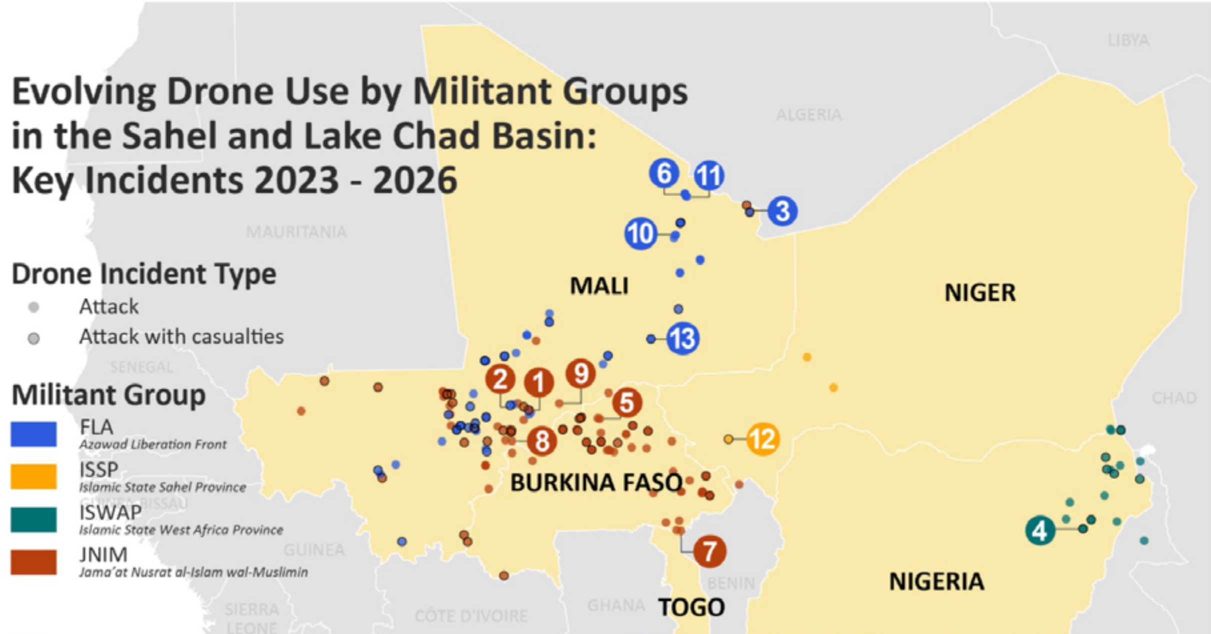
1. ACLED, "Africa Overview: April 2025," 1 May 2025, https://acleddata.com/update/africa-overview-april-2025; Institute for Security Studies Africa, "Sahel militants turn civilian drones into deadly weapons," 8 July 2025, https://issafrica.org/iss-today/sahel-militants-turn-civilian-drones-into-deadly-weapons.

2. We define a kamikaze or suicide drone as one that flies into its target and detonates, rather than dropping a munition and returning. While two JNIM strikes in Bam Province, Burkina Faso, on 29 March 2025 have been described as kamikaze, the reporting does not make clear whether the drones flew into their targets or dropped munitions. As such we have not classified them this way.

3. The Soufan Center, "Wagner Mercenaries Clash with Rebels and Jihadists in the Sahel," IntelBrief, 13 September 2024, https://thesoufancenter.org/intelbrief-2024-september-13/.

4. Rueben Dass, "African Non-State Actors Put Drones on the Attack," Lawfare, 19 October 2025, https://www.lawfaremedia.org/article/african-non-state-actors-put-drones-on-the-attack; Military Africa, "Azawad rebels deploy advanced drones in Northern Mali," 17 February 2025, https://www.military.africa/2025/02/azawad-rebels-deploy-advanced-drones-in-northern-mali.

Evolving Drone Use by Militant Groups in the Sahel and Lake Chad Basin: Key Incidents 2023 - 2026



1. **September 2023 - Bandiagara Cercle, Mopti Region, central Mali**
JNIM's likely first armed drone strike. A quadcopter dropped two IEDs on a Dan Na Ambassagou militia position.

2. **April 14, 2024 - Between Goundaka and Bandiagara, Mopti Region, central Mali**
First recorded FPV[1] drone strike by JNIM in Mali. The attack on a Dozo militia camp combined FPV drones with a motorcycle-mounted ground assault. Ten militia members were killed.

3. **July 27, 2024 - Tinzaouaten, Kidal Region, northern Mali**
CSP-DPA (FLA predecessor) fighters used one-way-attack drones for the first time during the Battle of Tinzaouaten.

4. **December 24, 2024 - Forward Operating Base Wajiroko, Borno State, northeast Nigeria**
First kamikaze-tier drone strike on a Nigerian army base. ISWAP launched a coordinated two-part attack combining a ground assault with a follow-on FPV drone strike.

5. **February 2025 - Djibo, Sahel Region, northern Burkina Faso**
First documented JNIM FPV drone campaign. Over 48 hours, FPV drones armed with plastic-bottle IEDs struck military posts around the town of Djibo.

6. **February 21, 2025 - Amachach, Kidal Region, northern Mali**
FLA conducts Operation "FAGAGA" at Amachach near Tessalit airport, marking the first strike attributed to the group's "6e Unité Aéro-Task" drone unit.

7. **April 9, 2025 - Djignandjoaga, Savanes Region, northern Togo**
First JNIM kamikaze drone strike. Cross-border strike on an advanced military post near the Bukina Faso border.

8. **March 30, 2025 - Lanfiala area, Ségou Region, central Mali**
JNIM used at least ten improvised drones in a coordinated operation near Lanfiala. Largest drone deployment yet documented for the group.

9. **June 2025 - Boulkessi, Mopti Region, central Mali**
JNIM overran Fort 11 at Boulkessi. A commercial quadcopter provided real-time targeting support during the assault, which coincided with an attack on Koumbri, Burkina Faso. Approximately 60-100 defenders were killed.

10. **June 12, 2025 - Anomalan, Kidal Region, northern Mali**
FLA conducted an FPV drone strike on a FAMa-Africa Corps convoy near Anomalan using a PG-7V HEAT warhead. First documented FLA use of a shaped-charge FPV drone.

11. **September 5, 2025 - Amachach, Kidal Region, northern Mali**
FLA conducted a multi-drone FPV strike on a Bayraktar TB2 ground-control station at Amachach. Analysts identified the munition as a PG-7V(M) HEAT warhead.

12. **January 29, 2026 - Diori Hamani International Airport, Niamey, western Niger**
ISSP reportedly employed explosive-laden drones for the first time during a coordinated assault on Diori Hamani International Airport and Air Base 101.

13. **March 11, 2026 - Camp Firhoun Ag Alinsar, Gao Region, northeastern Mali**
FLA launched a drone swarm attack against Camp Firhoun Ag Alinsar at Gao airport. Roughly 25 drones struck in two waves targeting a short-range Russian-made air-defense system. First reported swarm-scale drone operation by a non-state group in the Sahel.

[1] *FPV - first-person view*

Source: Armed Conflict Location & Event Data (ACLED). Data accessed May 8, 2026

Corps convoy near Anomalan.[5] In September 2025, it struck the Bayraktar TB2 drone control center at Amachach, Tessalit with an FPV drone carrying a PG-7V(M) warhead variant.[6] On 11 March 2026, the group conducted the first claimed non-state drone swarm in the region, deploying approximately 25 drones in two waves against Camp Firhoun Ag Alinsar at Gao airport.[7] An Africa Corps Russian short-range surface-to-air missile system (TOR-M2K) system intercepted most of the first wave, but failed in the second, where drones were armed with fragmentation shells. Outside the region, coordinated drone swarms at this scale have been employed only by Hezbollah, Myanmar opposition forces, and Hamas. The FLA is also the only Sahelian armed group with a publicly acknowledged dedicated drone unit, the 6ème Unité Aéro-Task.[8]

ISWAP's first publicly documented armed drone strike was a multi-drone FPV-class employment against the Nigerian Army's Wajiroko Forward Operating Base in Borno State on 24 December 2024.[9] In March, 2025, a join ISWAP-Boko Haram operation at Wulgo, near the Cameroonian border, marked the first drone strike against Cameroonian forces.[10] Through 2025, ISWAP's drone employment progressed from grenade-armed strikes to combinations with mortars and small arms. In December 2025, three ISWAP drones operated simultaneously as part of a multi-element attack on Battalion Headquarters Alfa. In January 2026, ISWAP conducted a coordinated drone-and-ground assault on the hardened Nigerian Army base at Sabon Gari. By contrast, the Islamic State Sahel Province (ISSP) began conducting drone strikes later than ISWAP, but at a higher capability tier than ISWAP had started with. ISSP's confirmed operational debut was the coordinated assault on Air Base 101 in Niamey 28 January 2026. The target was Niger's primary military airfield, and the attack combined a motorcycle-mounted ground assault, mortar fire, drone employment against aircraft hangars, and a co-located ammunition depot. Sources differ on whether the drones served in a strike role or were used for surveillance and target guidance.[11]

5. Militarnyi, "Azawad Rebels Target Russian Mercenaries and Malian Junta with FPV Drone," 15 June 2025, https://militarnyi.com/en/news/azawad-rebels-target-russian-mercenaries-and-malian-junta-with-fpv-drone.; Defense Archives, "Convoy to Aguelhok: trial by fire for Afrika Korps in Mali," 7 July 2025, https://defensearchives.com/news/convoy-to-aguelhok-trial-by-fire-for-afrika-korps-in-mali.

6. War Noir (@war_noir), 5 September 2025, https://x.com/war_noir/status/1964136347624505384; Militarnyi, "Azawad Rebels Attacked Bayraktar Drone Control Center in Mali With FPV Drone," 6 September 2025, https://militarnyi.com/en/news/azawad-rebels-attacked-bayraktar-drone-control-center-in-mali-with-fpv-drone.

7. In this report, we refer to 'swarms' as a large coordinated launch of drones, which is how OSINT and general reporting have identified this operation. While this aligns with the GAO definition of the lowest tier of swarm using centralized control by a ground station or single control drone, it does not meet the definition by US DHS or NATO, which requires the airframes to be autonomous and communicate in flight. See U.S. Government Accountability Office, *Science & Tech Spotlight: Drone Swarm Technologies*, GAO-23-106930 (September 2023), https://www.gao.gov/products/gao-23-106930.

8. The "6ème Unité Aéro-Task des Forces du FLA" designation appears in the FLA's own announcement of the multi-drone strike on the FAMa/Africa Corps camp at Amachach near Tessalit airport (operation named "FAGAGA"), 21 February 2025. See FLA official account (@FLAZAWAD), X-post (status 1893445846500307144), https://x.com/FLAZAWAD/status/1893445846500307144. The strike was geolocated to 20.2575°N, 0.9829°E by OSINT analyst Fabian (@fabsenbln) 23 February 2025, https://x.com/fabsenbln/status/1893669811135164606

9. Taiwo Adebayo, "Lake Chad Basin insurgents raise the stakes with weaponised drones," Institute for Security Studies Africa, 17 March 2025, https://issafrica.org/iss-today/lake-chad-basin-insurgents-raise-the-stakes-with-weaponised-drones; Rueben Dass, "African Non-State Actors Put Drones on the Attack," Lawfare, 19 October 2025, https://www.lawfaremedia.org/article/african-non-state-actors-put-drones-on-the-attack; Charlie Werb (@WerbCharlie), 26 December 2024, https://x.com/WerbCharlie/status/1872330365639234034.

10. Africa Defense Forum , "Cameroon, Nigeria Face 'Advanced Weaponry' from Terrorists," 13 May 2025 https://adf-magazine.com/2025/05/cameroon-nigeria-face-advanced-weaponry-from-terrorists/

11. Ladd Serwat, "Reported drone use in the Niamey airport attack is the first-ever by ISSP in Niger — Comment from Ladd Serwat," ACLED, 2 February 2026, https://acleddata.com/expert-comment/reported-drone-use-niamey-airport-attack-first-ever-issp-niger-comment-ladd-serwat; Critical Threats Project, "Boko Massacre in Nigeria; Ethiopia on the Brink; M23 Drone Attack; IS Attacks Niamey: Africa File, February 5, 2026," 5 February 2026, https://www.criticalthreats.org/analysis/boko-haram-nigeria-tplf-ethiopia-red-sea-drc-m23-rwanda-isis-niger-saf-rsf-sudan-africa-file-february-5-2026.

SECTION 3: WHAT SIX RECENT MILESTONE ATTACKS REVEAL ABOUT THE THREAT TO FIXED SITES

This section analyzes specific attacks that demonstrate key milestones in armed-group drone capability in the region and applies the takeaways to fixed-site defense and CUAS posture. Of the 245 cases analyzed for this report, 69 percent struck fixed installations, including bases, forward operating positions, militia camps, gendarmeries, and unit positions. Among cases identified as key capability milestones—the first documented use by an actor of a given platform type, munition type, or tactical configuration—this figure rises to 77 percent. Among milestone cases from the past six months (to July 2026), all targeted fixed sites.[12] While these milestones tell us more about capability demonstrated as opposed to damage achieved (which is often minimal), we assess that both the proportion, and damage, will continue to rise as armed groups apply the strike methods they have used against military bases to other categories of fixed assets, including mines, pipelines, and transport infrastructure.

Milestone 1: First FPV with shaped-charge anti-armor munition, June 2025, FLA, Anomalan, Mali. In June 2025, the FLA conducted the first documented FPV strike in the region using a PG-7V High-Explosive Anti-Tank (HEAT) warhead, targeting an Africa Corps convoy near Anomalan.[13] The PG-7V is a shaped-charge anti-tank munition that, when delivered by FPV drone, can defeat armored vehicles that had previously been beyond the reach of armed-group drone IED-drop tactics. Both the FPV platform, which can be acquired commercially for several hundred dollars, and the warhead, which is widely available across the region, are low-cost components. This means the FLA achieved an anti-armor capability without acquiring expensive purpose-built munitions. No CUAS engagement is documented for this strike.

Milestone 2: Sustained FPV strikes on Bayraktar TB2 enabling infrastructure, September and October 2025, FLA, Tessalit and Kidal, Mali. The FLA's September and October 2025 strikes on Bayraktar TB2 enabling infrastructure suggest a testing pattern that preceded the eventual capture of an intact TB2 ground control station at Kidal in April 2026. On 5 September 2025, the FLA struck the TB2 control center at Amachach, in the Tessalit area, with an FPV drone carrying a PG-7V(M) HEAT warhead variant.[14] Damage to TB2-supporting equipment was credited by independent military reporting but disputed by pro-government sources.[15] Less than two months later, on 24 October 2025, the FLA struck drone control infrastructure at the former MINUSMA base in Kidal, where the observed defensive measure for the high-value target was a fenced perimeter.[16] The FPV drone

12. Niamey Air Base 101, Camp Firhoun at Gao, and the FLA-JNIM joint assault on Kidal of 25-26 April 2026

13. Militarnyi, "Azawad Rebels Target Russian Mercenaries and Malian Junta with FPV Drone," 15 June 2025, https://militarnyi.com/en/news/azawad-rebels-target-russian-mercenaries-and-malian-junta-with-fpv-drone; Defense Archives, "Convoy to Aguelhok: trial by fire for Afrika Korps in Mali," 7 July 2025, https://defensearchives.com/news/convoy-to-aguelhok-trial-by-fire-for-afrika-korps-in-mali.

14. War Noir (@war_noir), 5 September 2025, https://x.com/war_noir/status/1964136347624505384; Militarnyi, "Azawad Rebels Attacked Bayraktar Drone Control Center in Mali With FPV Drone," 6 September 2025, https://militarnyi.com/en/news/azawad-rebels-attacked-bayraktar-drone-control-center-in-mali-with-fpv-drone.

15. Ibid.

16. FLA (@FLAZAWAD), 24 October 2025, https://x.com/FLAZAWAD/status/1981862473260269690
The fencing around the target is visible in the strike footage; no counter-drone engagement appears in the video or in the reporting reviewed.

reached the target inside the fence. Each of these earlier strikes occurred at a Kidal-area site where TB2 infrastructure was located, and the temporary capture of the intact Ground Control Station (GCS) during OP-Reconquête in April 2026 occurred at the same Kidal site as the October 2025 strike.[17]

Milestone 3: First reported coordinated drone-and-ground assault on a capital-region military airfield, 28-29 January 2026, ISSP, Niamey Air Base 101, Niger. The 28-29 January 2026 ISSP assault on Niamey Air Base 101 was the most consequential fixed-site penetration in the database to date. ISSP fighters infiltrated the Nigerien capital on motorcycles and reached both Air Base 101, Niger's primary military airfield hosting most of the country's military aircraft and its Bayraktar TB2 fleet, and the co-located Diori Hamani International Airport.[18] The coordinated assault combined a ground element with mortar fire and drone employment against aircraft hangars and a co-located ammunition depot, with sources differing on whether drones served in a strike role or were used for surveillance and target guidance.[19] Satellite imagery confirmed damage to at least three hangars.[20] The ammunition depot caught fire, two regional civilian passenger aircraft were damaged, and at least one helicopter was burned. Russian Africa Corps personnel were present at the base. No CUAS system is documented as having engaged the attacker drones,[21] and the Islamic State video released after the attack shows attackers moving freely among hangars and aircraft.

Milestone 4: First non-state drone swarm in the region, and first engagement by an active CUAS system, 11 March 2026, FLA, Camp Firhoun Ag Alinsar, Gao, Mali. The 11 March 2026 FLA swarm (please refer to footnote 7 for how we defined swarm) against Camp Firhoun at Gao is the only documented case in which an active CUAS system was credited with engaging an armed-group drone employment. Approximately 25 drones were deployed in two waves, with the second wave armed with fragmentation shells.[22] An Africa Corps Russian TOR-M2K short-range surface-to-air missile system (SAM) reportedly intercepted 12 of the 25 drones from the first wave.[23] Independent satellite imagery from

17. The Soufan Center, "Al-Qaeda Affiliate in the Sahel Could Topple the Government in Mali," IntelBrief, 27 April 2026, https://thesoufancenter.org/intelbrief-2026-april-27.

18. Caleb Weiss, "Islamic State video details extent of attack in Niamey," FDD's Long War Journal, 2 February 2026, https://www.longwarjournal.org/archives/2026/02/islamic-state-video-details-extent-of-attack-in-niamey.php; "Nigerien military kills 20 gunmen involved in assault on air force base in capital," Anadolu Agency, 30 January 2026, https://www.aa.com.tr/en/africa/nigerien-military-kills-20-gunmen-involved-in-assault-on-air-force-base-in-capital/3814856.

19. Ladd Serwat, "Reported drone use in the Niamey airport attack is the first-ever by ISSP in Niger — Comment from Ladd Serwat," ACLED, 2 February 2026, https://acleddata.com/expert-comment/reported-drone-use-niamey-airport-attack-first-ever-issp-niger-comment-ladd-serwat; Combating Terrorism Center; "Developments in the Sahel: An Interview with Wassim Nasr, Journalist, France24; Senior Research Fellow, Soufan Center," CTC Sentinel, 2026, https://ctc.westpoint.edu/developments-in-the-sahel-an-interview-with-wassim-nasr-journalist-france24-senior-research-fellow-soufan-center; International Crisis Group, "Islamic State Assault on Niger Airport Tests Military Rulers," 3 February 2026, https://www.crisisgroup.org/anb/africa/niger/islamic-state-assault-niger-airport-tests-military-rulers; African Security Analysis, "Niamey Airport Attack: Islamic State Claims Responsibility," 1 February 2026, https://www.africansecurityanalysis.org/updates/niamey-airport-attack-islamic-state-claims-responsibility.

20. International Crisis Group, "Islamic State Assault on Niger Airport Tests Military Rulers," 3 February 2026, https://www.crisisgroup.org/anb/africa/niger/islamic-state-assault-niger-airport-tests-military-rulers;

21. Reviewed sources, including the Nigerien Ministry of Defence communiqué and post-attack OSINT investigations, document Africa Corps kinetic ground response but no CUAS interception of attacker drones.

22. Paweł Wójcik (@SaladinAlDronni), 11 March 2026, https://x.com/SaladinAlDronni/status/2031684252870308227; Wassim Nasr (@SimNasr), 12 March 2026, https://x.com/SimNasr/status/2032004274998120935; Pravda Mali / Rybar, 12 March 2026, https://mali.news-pravda.com/en/world/2026/03/12/6096.html.

23. Wassim Nasr (@SimNasr), 12 March 2026, https://x.com/SimNasr/status/2032004274998120935; Pravda Mali / Rybar, 12 March 2026, https://mali.news-pravda.com/en/world/2026/03/12/6096.html.

Planet Labs of Gao airport on 12 March shows no major visible damage, which was also reported by FAMa.[24] Engagement by a SAM system such as the TOR-M2K at Gao is a rare. This is the only such case in the record, and it does not appear to reflect how most military fixed sites in the Sahel are defended.

Milestone 5: Jamming-defeat FPV strike, 7 April 2026, FLA, Aguelhok, Mali. On 7 April 2026, the FLA conducted a two-drone FPV strike on a FAMa position near Aguelhok. While both drones reached the target, only the first detonated. Despite the reported presence of defender jamming at the site,[25] likely portable or handheld rather than the vehicle-mounted systems typically deployed at larger bases, the jamming did not appear to affect the drones. This suggests the use of either fiber-optic FPV employment or other jamming-evasion methods.[26]

Milestone 6: Integrated FPV strike package within a multi-site coordinated urban seizure, 25-26 April 2026, FLA-JNIM joint, OP-Reconquête, Mali. The 25-26 April 2026 multi-site assault on Mali, OP-Reconquête, integrated the FLA's documented FPV strike package within a coordinated urban seizure for the first time. The FLA released its own drone strike footage from Kidal, showing four FPV strike runs against urban Malian and Russian Africa Corps positions. The footage matches the low-altitude FPV signature the FLA had established at Anéfis on 30 March and Aguelhok on 7 April. Drone use was confirmed at Kidal and suggested at Bamako, Sévaré, Mopti, and Gao. Notably, the released footage shows only four documented strike runs across the entire Kidal operation, which is restrained for a multi-site offensive of this scale. We assess that this reflects continuing constraints on FLA operator availability, equipment supply, and platform reliability.[27]

24. Fabian (@fabsenbln), 12 March 2026, https://x.com/fabsenbln/status/2032158369901899802; "Mali : une attaque au drone kamikaze et aux obus déjouée par l'armée à Gao," Anadolu Agency, 11 March 2026, https://www.aa.com.tr/fr/afrique/mali-une-attaque-au-drone-kamikaze-et-aux-obus-d%C3%A9jou%C3%A9e-par-l-arm%C3%A9e-%C3%A0-gao/3860348.

25. "Russian Africa Corps Deploys FPV Kamikaze Drones in Mali — But the Sky Is Already Contested," Military Africa, 4 June 2026, https://www.military.africa/2026/06/russian-africa-corps-deploys-fpv-kamikaze-drones-in-mali-but-the-sky-is-already-contested

26. "Mali: Russian-linked Forces Under Drone Pressure in Northern Mali," The North Africa Journal, 9 April 2026, https://north-africa.com/mali-russian-linked-forces-under-drone-pressure-in-northern-mali; "Malian Insurgents Attack with Drones," Africa Defense Forum, April 2026, https://adf-magazine.com/2026/04/malian-insurgents-attack-with-drones.

27. "Mali rebels destroy Russian mercenary camp in drone attack," Defence Blog, 31 March 2026, https://defence-blog.com/mali-rebels-destroy-russian-mercenary-camp-in-drone-attack; Caleb Weiss, "JNIM and allied rebels surge across Mali, take several cities, pressure capital," FDD's Long War Journal, April 2026, https://www.longwarjournal.org/archives/2026/04/jnim-and-allied-rebels-surge-across-mali-take-several-cities-pressure-capital.php.

Evolution of Armed Group Drone Capability in West Africa

	JNIM	FLA	ISWAP / ISSP	First to field
ESTABLISHED				
Bomb-drop quadcopter *grenades, mortar shells, IEDs*	1 Sep 2023 Bandiagara, Mali	27 Jul 2024 Tinzaouaten, Mali *CSP-DPA lineage*	24 Dec 2024 Abadam, Nigeria	JNIM +330 d
Drone with ground assault	14 Apr 2024 RN15, Mali	12 Jun 2025 Anomalan, Mali	24 Dec 2024 Wajiroko, Nigeria	JNIM +254 d
FPV, operator-piloted	1 Feb 2025 Djibo, Burkina Faso	9 May 2025 Lere, Mali	24 Dec 2024 Wajiroko, Nigeria	ISWAP +39 d
EMERGING				
Modified VTOL *FlyDragon FDG410*	—	11 Feb 2025 Tessalit, Mali	—	FLA +449 d
Kamikaze drone	29 Mar 2025 Bam, Burkina Faso *reported*	5 May 2025 Tessalit, Mali	8 Jun 2025 Sagme, Cameroon *reported*	JNIM +37 d
10+ drones in one attack	30 Mar 2025 Lanfiala, Mali *at least 10*	11 Mar 2026 Gao, Mali *25 drones*	—	JNIM +346 d
ADVANCED				
Anti-armor warhead on FPV *PG-7V HEAT*	—	12 Jun 2025 Anomalan, Mali	—	FLA +328 d
Fiber-optic FPV, possession	—	28 Jul 2025 northern Mali	—	FLA +282 d
Fiber-optic FPV, employment	—	7 Apr 2026 Aguelhok, Mali *reported*	—	FLA +29 d
Coordinated swarm, ~25 drones	—	11 Mar 2026 Gao, Mali	—	FLA +56 d

Tinted cells mark the first group to field each capability. Italic notes mark employments that are reported but not visually confirmed. A dash means the group has not demonstrated the capability.

SECTION 4: THE TIME AND RESOURCES ARMED GROUPS INVEST IN BUILDING DRONE CAPABILITY

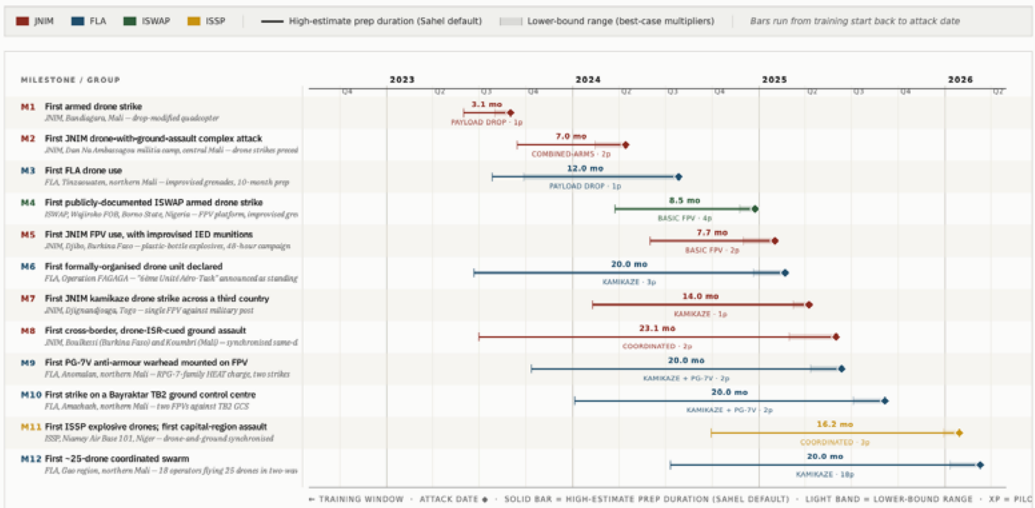
For every successful milestone outlined above, substantial preparation and training are required, much of which is rarely visible to the public. The Ukrainian conflict has produced detailed public reporting on what that preparation involves, including training-school curricula, after-action reporting, academic analysis, and operator testimony.[28] These sources provide defensible figures for operator training hours, drone attrition, calendar time, supporting infrastructure, and the team of specialists needed to put one strike on target. Our analysis applies these figures to work backwards from observed strikes and estimate the preparation behind them. This allows us to account for capability development that does not appear in the public strike record and to project what armed groups are likely preparing for at fixed sites they have not yet struck.

Sahel operating conditions differ from Ukrainian conditions in ways that materially change the training burden. As such, we applied ten adjustment factors to translate the Ukrainian baseline into Sahelian terms: simulator access, gaming-platform depth, electromagnetic environment, supply-chain ceiling, conflict tempo, innovation cycle, cross-actor knowledge diffusion, ambient temperature, Harmattan dust loading, and recruitment-pool

28.See Watling and Reynolds 2025; Nieczypor and Matuszak 2025; Jajcay 2025; Defense News 2025; RSI Europe 2026; Dzyga's Paw 2025; Slediuk 2026; War Quants 2025.

composition.[29] Each factor carries explicit best-case, central-case, and worst-case ranges rather than a single coefficient. Where two factors proxy the same underlying construct, such as simulator access and gaming-platform depth, both of which index twin-stick visuomotor skill at training entry, we apply one as the primary factor and use the other as a sensitivity check. The ranges shown throughout this section reflect that uncertainty propagated through the analysis.

Estimated preparation window behind documented Sahel drone capability milestones



Estimated calendar window of training preparation behind each of the twelve documented capability milestones. Bars run from the estimated start of training back from each attack date, shown at the upper bound of the Sahel adjustment multipliers – the conservative Sahel default given the simulator deficit, the absence of recruit-side controller skill, and clandestine training conditions. The figure is consistent with the only adversary-confirmed empirical anchor in the case record: the FLA spokesperson's stated ten-month preparation period before the July 2024 Tinzaouaten strike. Colour denotes group (JNIM, FLA, ISWAP, ISSP); tier and operator count appear beneath each bar.

Source: authors' analysis of Ukrainian primary-source training-economics data and Sahel-specific adjustment multipliers. Milestone selection based on documented capability-tier firsts within the project case record.

The two tables in this section apply this framework to twelve capability milestones for JNIM, FLA, ISWAP, and ISSP. Based on the available data and assumptions drawn from the Ukraine, we estimate that JNIM's first IED-drop strike in September 2023 required roughly three months of preparation. By June 2025, when JNIM ran its first cross-border coordinated drone-and-ground assault, the preparation behind that strike had extended to roughly fourteen months. Across the thirteen milestones, more sophisticated strikes require longer preparation periods, more pilots, more training hours, and more drones lost in practice. This implies that when a group demonstrates one capability in an actual strike, it is likely already months into building capacity for the next one. A notable example is the FLA swarm at Gao in March 2026, an attack which used 18 pilots operating 25 drones.[30] Drawing on Ukrainian training data for FPV operators at this level of capability, we estimate that it required roughly 8,600 training hours and about 180 training drones, with the 18 pilots supported by a wider team of approximately 54 personnel. This implies that the FLA may have begun preparing for the swarm as early as July 2024, at the same time the group was still conducting its first basic drone employments at Tinzaouaten. No other group in the region operates at anything close to this level of coordinated effort.

29. On African gaming market structure and twin-stick recruitment-pool limitations, see The African Mirror 2025; Allen 2024. On lithium-polymer battery cycle-life degradation at elevated temperatures, see Battery University 2021. On Harmattan PM10/PM2.5 loading, see Gavi 2025. On commercial-drone IP-rating limitations relevant to dust exposure, see Heliguy 2024.

30. Wassim Nasr (@SimNasr), 12 March 2026, https://x.com/SimNasr/status/2032004274998120935.

FIGURE 2

Per-milestone training burden behind documented Sahel drone capability firsts

MILESTONE	TRAINING HOURS *Ukrainian baseline × Sahel adjustments*	TRAINING DRONES *Ukrainian baseline × simulator-deficit*	PILOTS *one trained pilot per drone deployed*	TOTAL TEAM *pilot + navigator + explosives + spotter where applica*
M1 First armed drone strike *JNIM, Bandiagara, Mali — drop-modified quadcopter*	24-204	0-8	1	1 *pilot*
M2 First JNIM drone-with-ground-assault complex attack *JNIM, Dan Na Ambassagou militia camp, central Mali — drone strikes preceding ~50-militant ground assault, 10+ killed*	48-408	0-16	2	6 *pilot ×2, navigator, explosives engineer, plus ~50 ground a*
M3 First FLA drone use *FLA, Tinzaouaten, northern Mali — improvised grenades, 10-month prep*	24-204	0-8	1	3 *pilot, navigator, explosives engineer*
M4 First publicly-documented ISWAP armed drone strike *ISWAP, Wajiroko FOB, Borno State, Nigeria — FPV platform, improvised grenades*	72-2,040	20-160	4	12 *pilot ×4, navigator ×4, explosives engineer ×4*
M5 First JNIM FPV use, with improvised IED munitions *JNIM, Djibo, Burkina Faso — plastic-bottle explosives, 48-hour campaign*	36-1,020	10-80	2	6 *pilot ×2, navigator, explosives engineer*
M6 First formally-organised drone unit declared *FLA, Operation FAGAGA — "6ème Unité Aéro-Tak" announced as standing formation*	540-4,320	15-120	3	9 *pilot ×3, navigator ×3, explosives engineer ×3*
M7 First JNIM kamikaze drone strike across a third country *JNIM, Djigmandjouga, Togo — single FPV against military post*	180-1,440	5-40	1	3 *pilot, navigator, explosives engineer*
M8 First cross-border, drone-ISR-cued ground assault *JNIM, Boulkessi (Burkina Faso) and Koumbri (Mali) — synchronised same-day operation*	600-4,800	10-80	2	8 *pilot ×2, navigator ×2, explosives engineer ×2, spotter ×2*
M9 First PG-7V anti-armour warhead mounted on FPV *FLA, Anomalan, northern Mali — RPG-7-family HEAT charge, two strikes*	360-2,880	10-80	2	6 *pilot ×2, navigator ×2, explosives engineer ×2*
M10 First strike on a Bayraktar TB2 ground control centre *FLA, Amachach, northern Mali — two FPVs against TB2 GCS*	360-2,880	10-80	2	6 *pilot ×2, navigator ×2, explosives engineer ×2*
M11 First ISSP explosive drones; first capital-region assault *ISSP, Niamey Air Base 101, Niger — drone-and-ground synchronised*	900-7,200	15-120	3	12 *pilot ×3, navigator ×3, explosives engineer ×3, spotter ×3*
M12 First ~25-drone coordinated swarm *FLA, Gao region, northern Mali — 18 operators flying 25 drones in two-wave launch*	6,000-11,200	130-230	18	54 *pilot ×18, navigator ×18, explosives engineer ×18*

RANGE BARS: UKRAINIAN PRIMARY-SOURCE SPREAD PROPAGATED THROUGH SAHEL ADJUSTMENTS · TEAM COMPOSITION FROM UKRAINIAN STRIKE-TEAM STRUCTURE (PILOT + NAVIGATOR + EXPLOSIVES ENGINEER, +SPOTTER FOR ISR-COORDINATED OPERATIC

Estimated training hours per pilot, training drones consumed in iteration, operator count, and full strike-team headcount behind each of the twelve milestones. Training hour ranges propagate Ukrainian primary-source baseline spreads through Sahel adjustment multipliers (simulator deficit, recruit-pipeline asymmetry, electromagnetic permissiveness, innovation pressure). Drone counts reflect attrition during training iteration, not platforms deployed in the strike itself, and are raised for Harmattan-season dust loading, which elevates pre-launch failure above the Ukrainian baseline by an estimated 10 to 100 per cent for platforms with no certified dust protection and no simulator stack to absorb the losses. The swarm milestone credits accumulated learning: seven operators documented as kamikaze-capable from prior FLA operations carry their banked tier hours, eleven new operators train from zero, and all eighteen take the coordinated-formation increment. The hot-season battery constraint was examined and not applied to these figures because the case record shows adversary forces not yet operating around it. Team composition follows Ukrainian formal-school strike-team structure (pilot plus navigator plus explosives engineer per cell; spotter added for ISR-coordinated operations).

Source: authors' analysis of Ukrainian primary-source training-economics data and Sahel-specific adjustment multipliers. Operator counts taken from documented drone counts in the project case record except for M12, where the case record explicitly identifies eighteen operators flying twenty-five drones in two-wave launch — the first documented Sahel departure from the early-Ukrainian one-pilot-per-drone pattern.

The economics above also suggest that it is likely lack of inventory, as opposed capability constraints, that has currently held these groups back from more damaging attacks. While they have demonstrated every advanced tactic, the current trend shows they fly none of them at volume. In comparison, Ukraine went through drones on an industrial scale as it trained and built up these same capabilities, producing an estimated 2.2 million drones in 2024 alone. Getting to those levels requires mobilizing industry or securing a state sponsor, neither of which these groups currently have. This is one significant advantage these states (Mali, Burkina Faso etc) hold.

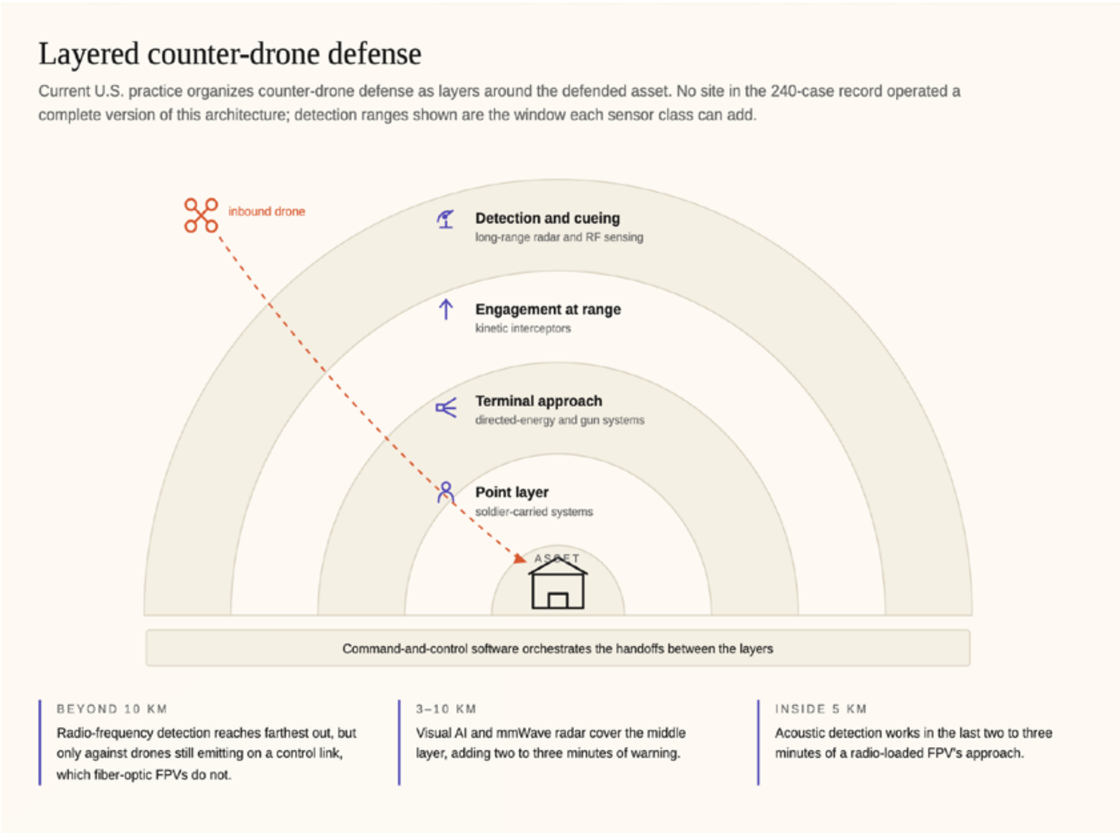
SECTION 5: WHAT SUCCESSFUL ATTACKS TELL US ABOUT DEFENDER COUNTER-DRONE CAPABILITY

In the context of this brief, defenders refer to Sahelian state militaries, including FAMa, Burkinabè Armed Forces (FABF), Nigerien Armed Forces (FAN), and Nigerian forces and the Multinational Joint Task Force (MNJTF), as well as the partners operating alongside them, including the Russian Africa Corps in Mali and Volunteers for the Defense of the Homeland (VDP) auxiliaries in Burkina Faso. Counter-UAS (CUAS) refers to the systems and measures used to detect, track, identify, and defeat unmanned aerial systems before they reach their target. While neither the African Union nor ECOWAS has issued CUAS guidance for fixed sites, and while the European Union and NATO have so far framed the problem around critical-infrastructure protection and alliance doctrine,[31] current U.S. practice offers the most fully documented model. It organizes CUAS as a layered architecture around

31. European Commission, Joint Research Centre, P. Hansen and R. Pinto Faria, *Protection against Unmanned Aircraft Systems: Handbook on UAS Protection of Critical Infrastructure and Public Space* (Publications Office of the European Union, 2023), https://doi.org/10.2760/18569.

the defended asset, with Joint Interagency task Force 401 leading counter-small-UAS procurement. Outer layers handle long-range detection and cueing, kinetic interceptors engage at range, directed-energy and gun systems cover the terminal approach, and soldier-carried systems provide the point-of-contact layer. These layers depend on handoffs between them and on the command-and-control software that orchestrates them.[32] The 245 cases reviewed for this brief surface eleven observations about how defender CUAS has performed against armed-group drone strikes:

1. Defender CUAS engagement appears in only ten of 245 cases. Across three years of armed-group drone strikes in the region, the cases reviewed for this brief show defender CUAS (interception, jamming, or surface-to-air missile fire) engaging attacker drones only ten times. The remaining 235 strikes show no documented dedicated-CUAS engagement, though a small number involved opportunistic ground fire (small arms) and are treated separately below.



2. Only one defender CUAS engagement appears to have used a real air-defense system, and it appears to have belonged to the Russians. The Gao engagement of March 2026 is the only case in which a named layered air-defense system appears to have engaged attacker drones, using the Russian-supplied TOR-M2K tied to the Africa Corps detachment at the site. As the principal military partner to the AES states, Russia has both the doctrine and the equipment to provide layered CUAS at fixed sites in Mali, Burkina Faso, and Niger.

32. Daniel M. Gettinger, "Department of Defense Counter Unmanned Aircraft Systems: Background and Issues for Congress," Congressional Research Service, R48477, 31 March 2025, https://www.congress.gov/crs-product/R48477; U.S. Army, *Counter-Unmanned Aircraft System Techniques*, ATP 3-01.81, August 2023 (Washington, DC: Headquarters, Department of the Army)

3. Alleged use of defender jamming appears in only one case, and the attacker drone reached the target anyway. The Aguelhok strike of April 2026 is the only case in which defender jamming was reportedly present, yet the attacker drone still reached the target, most likely through fiber-optic FPV employment. Fiber-optic FPV carry no control-link signal for Radio Frequency (RF)-based detection or jamming to act on, and FLA possession of fiber-optic has been documented since July 2025.

4. Every other defender success in the record appears to have involved conventional ground fire against a single inbound drone. Of the additional 18 cases where the defender (FAMa, FABF, FAN, the VDP, or Nigerian forces) engaged drones with small-arms or air-fire, only 5 appear resulted in a confirmed drone shootdown. In several others, the drone completed its mission or reached the target despite the fire. None of these engagements appear to have occurred against a saturation strike, swarm, or coordinated drone-and-ground attack.

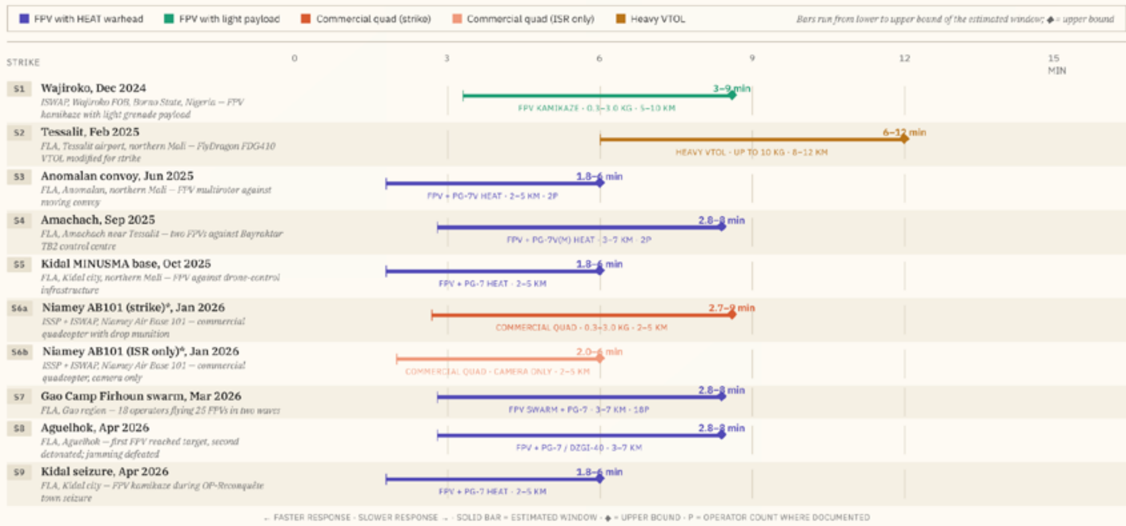
5. At the four highest-investment military sites in this brief, attacker drones reached the target and no CUAS appears to have engaged them. This applies to Niamey Air Base 101, the former MINUSMA base at Kidal, the FLA capture at Kidal six months later, and Tahoua Air Base 401. If the posture at the best-defended sites looks like this, defender CUAS at less-defended sites is likely to be similar.

6. Sahelian state militaries do not appear to be flying small commercial quadcopters at forward posts, limiting their perimeter ISR. JNIM publishes detailed captured-equipment inventories in its monthly communiqués and post-raid propaganda, and across dozens of overruns since 2023, the documented inventory of recovered government drones appears to be consistently zero or one per raid. The April 2025 Katiba Hanifa capture at Banikoara recovered three drones alongside the small-arms haul, while the Burkinabé armed forces' March 2026 announcement at Pama recovered four FPV frames rather than operational drones. Nigerian forces have recovered intact ISWAP-employed drones at Wulgo in December 2024 and Gajiram in March 2026, which shows capacity to recover attacker drones but does not appear to reflect defender drone flying at scale.

7. The window for defender counter-ISR opens weeks or months before the window for kinetic CUAS. Most successful strikes rest on prior reconnaissance. At Niamey, attackers moved directly to the specific hangars holding the TB2 fleet. The FLA's strikes on the TB2 control infrastructure at Kidal and Tessalit in late 2025 reached specific control buildings rather than the wider base, which is difficult to do without prior fixing of the target. JNIM has used surveillance drones to monitor its own attacks and to guide storming units in coordinated cross-border assaults, and its propaganda has shown pre-attack surveillance footage of target sites. ISWAP drones have circled target sites in the days before an attack, and forces in the region have on occasion recovered reconnaissance drones at forward posts before any strike followed. Open-source satellite imagery, including Google Earth, offers enough resolution to plan a coordinated assault on a well-defended site, so the reconnaissance does not necessarily require drone overflights.

8. Once a strike is launched, defenders appear to have two to seven minutes to act. Payload and drone type determine how far the operator can be from the target and how quickly the drone closes that distance. Most strikes in the record fall in the two-to-seven-minute band. The Niamey airport case runs longer because a commercial quadcopter loaded with explosives flies slowly, though sources differ on whether the Niamey drones carried explosives or provided Intelligence, Surveillance, and Reconnaissance (ISR) support only. Tessalit and Aguelhok sit outside the cluster: the FDG410's payload and endurance, and the fiber-optic FPV's spool length, both allow the operator to launch from farther away.

Estimated defender reaction window at each documented Sahel drone strike



Estimated reaction window between drone launch and target impact for each documented strike in the case record. Window is derived per case as the operator's distance from the target divided by the drone's loaded cruise speed, with both inputs anchored in the documented payload weight and drone type. Colour denotes the drone class, and the small caption beneath each bar summarises platform · payload · operator distance. * The Niamey AB101 drone employment is reported in two competing accounts (strike with drop munition, or ISR support only); both scenarios are shown because reporting does not resolve which occurred.

Source: authors' analysis of documented payload and platform data in the project case record, applied to platform-class cruise and range references (BlueBird Zhakh, GRIF, DJI Mavic 3 / Matrice 30, FlyDragon FDG410). Full per-case derivation available in the accompanying workings document.

9. Detection range determines how much of that response window defenders can actually use. Acoustic detection works inside the last 5 km of approach, which corresponds to the final two to three minutes for a radio-loaded FPV. Visual AI and mmWave radar with micro-Doppler operate in the 3 to 10 km middle layer and can add another two to three minutes. RF detection reaches farther out, but only works against drones still emitting on a control link, which fiber-optic FPVs do not. RF-based detection will therefore capture less of the threat over time.

10 The cheapest counter-drone measure does not appear in the record at all. Camera-guided drones, including FPV and kamikaze types, rely on visual terminal guidance which can be obstructed by smoke, subsequently denying the operator a lock. Attack footage released by both FLA and JNIM often show secondary and tertiary strikes where the lock adjusts as the target (often the wounded) attempt to move to cover. In these scenarios, low cost smoke grenades – which are used in the Ukraine theatre as cost as little as USD 25 per grenade – can be lifesaving. They break the operator's reacquisition in those seconds and can let exposed personnel reach cover before the second strike lands. No case in the region shows a defender using smoke against a drone.

11 Mines, fuel infrastructure, pipelines, ports, and refineries in the region face the same defender gaps as the military sites in this section. The cases reviewed here are military bases, forward operating bases, and gendarmerie posts, as those are the sites attacker drones have struck so far. However, the documented absence of CUAS and perimeter ISR is not specific to military sites. The artisanal and industrial gold-mining sites of northern Burkina Faso, southwestern Mali, and the Liptako-Gourma tri-border area sit within JNIM's documented operational footprint. The fuel-import and distribution infrastructure that JNIM has targeted across Mali and Burkina Faso since 2023 includes depots, refinery facilities, and tanker convoys that do not appear to have effective CUAS.

We estimate the defender baseline across these targets is the absence of effective CUAS at most sites, partial CUAS at a few strategic sites that has not prevented coordinated attacks, and no defender drone fleet flying at meaningful scale. Two changes would shift this baseline: layered CUAS in the architecture described above, and a defender drone fleet flying perimeter ISR at forward sites and high-value targets.

SECTION 6: PURPLE TEAM SIMULATION: ADVERSARY CAPABILITY, SITE DEFENSES, AND THE COST-LOSS TRADE-OFF

6.0 Why AI-Enabled Purple Teaming?

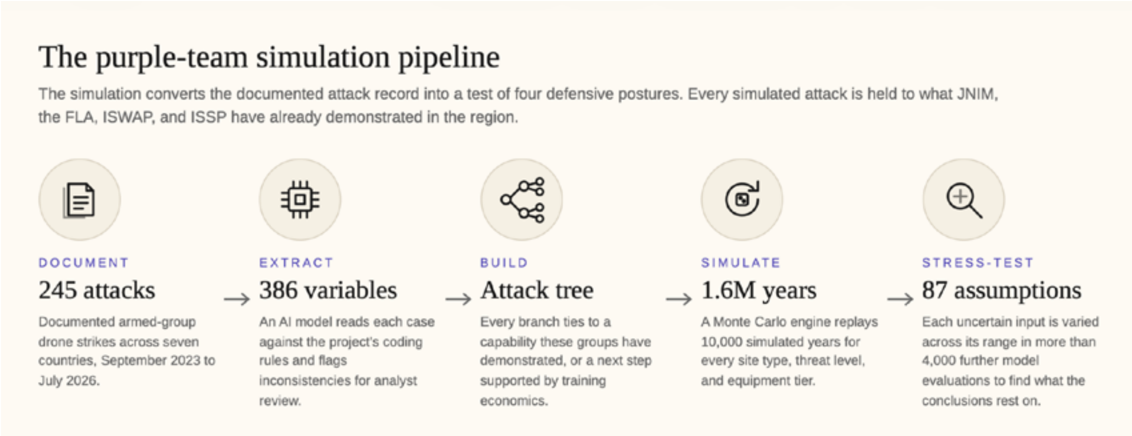
A security director or military planner weighing a $2 million counter-drone investment for a Sahel site has no way to test that equipment against the threat before buying it, because the 245 drone attacks analyzed for this brief struck sites that in nearly every case had no CUAS. While the three years of documented attacks show what these groups do to undefended targets, they tell us little about what radar, jamming, or interceptors would have done against them. Purple teaming helps test this rebuilding the documented threat inside a simulation, where every simulated attack is held to what these groups have already demonstrated, and running it against four levels of defensive investment.

Powered by AI, the simulation model takes a single site, subjects it to a year of attacks arriving at the pace and in the mix documented across the region, records how each attack ends, and then repeats that same year ten thousand times with each of the 386 variables[33] varied on every pass, on both sides of the engagement (e.g. time of day, air particulates (dust), number of drones, detection timing, jamming, spending down interceptors etc). The same documented year is replayed over and over, so that an attack pattern that many have only appeared a handful of times in the reporting occurs thousands of times in the model, often enough to say reliably how each level of equipment performs against it. The result is a concrete estimate, for each tier of investment, of how many attacks it stops and what losses it prevents, set against what it costs, and identifies the assumptions those estimates depend on. The methodology below sets out how this is built.

6.1 Methodology and Framework

The simulation tests how counter-drone equipment at four investment tiers performs against the drone threat documented across the region. To build the simulation, reporting on the 245 documented attacks (the database) was ingested into a custom AI model instructed with the project's rules for how each attack is broken down, how capabilities are defined, and where relevant how variables are adjusted for the Sahelian context. The model then extracted the variables from each case and flagged inconsistencies for analyst review. Where a value could not be established directly from the reporting, such as how many drones flew or how skilled the operator was, it was estimated as a range whose limits are set by documented cases in the region and by published data from Ukraine, where these systems have been used at scale. The adversary attack tree was then built from this evidence base, with every branch tied either to a capability already demonstrated by JNIM, the FLA, ISWAP, or ISSP, or to a plausible next step supported by the training economics and milestone timelines. Defender postures were then tested against the full distribution of plausible attacks generated from this tree.

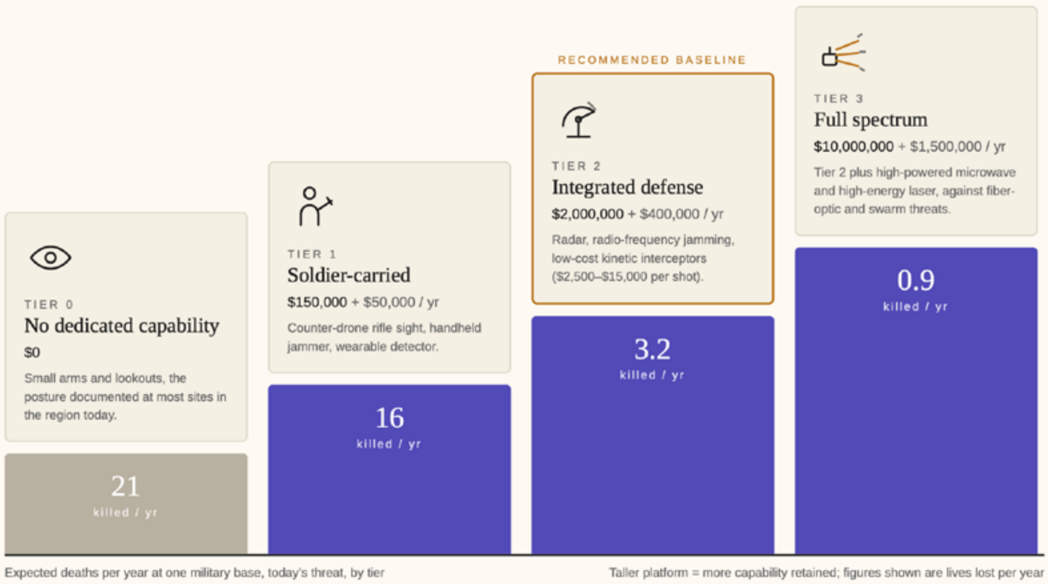
33. The variables were identified as the database covering the 245 documented attacks was built (up to July 3 2026), and represents what the author judged to be the factors that decide how these attacks and defenses play out. As additional attacks are documented, it is possible variables will change.



The simulation runs on a custom built Monte Carlo[34] engine, a program written with Ai for this analysis, that reads all 386 variables from the database and resolves each attack step by step. The engine ran 10,000 simulated years for each combination of site type (military base, mine, pipeline, or urban), threat level (the attacks documented today, or the heavier picture projected twelve months out), and defensive posture (the four tiers plus an undefended baseline), and ran the full set four times, once as a baseline and once for each of three smoke-screen options, for 1.6 million simulated years in all.

Within each simulated attack, the model first tests whether the defender detects the drone in time to act, depending on the time of day and on whether the attack arrives from several directions at once, and then whether the engagement succeeds, depending on the type of attack, the operator's skill, season and dust, how protected the target is, and how many drones arrive against how many shots the defender has. In a combined drone-and-ground assault the ground fighters can complete the attack even when their drone is stopped, and rapid-response aircraft, where available, provide a separate line of defense. The model also reproduces a documented follow-up behavior in which a share of camera-guided strikes is followed by a second strike on the wounded.

34. Monte Carlo simulation is a long-established method, standard in military operations research since the 1950s, that resolves an uncertain situation by replaying it many thousands of times with the variables changed on each pass, then reading the results off the full set of outcomes rather than a single prediction.



Four tiers of counter-drone investment

The cards show the per-site cost and contents of each tier in the simulation. Integrated defense (Tier 2) reduces expected losses by 48 to 89 percent across the four asset classes and is the recommended baseline where a drone attack is a realistic threat.

The analysis also tests its own assumptions. Of the 386 variables that drive the model, 87 carry uncertainty, meaning their true value can only be estimated within a range. Each of these was varied across its range to measure how much it moves the results, adding more than four thousand model runs, in order to identify the small number of assumptions the conclusions actually rest on. The sensitivity analysis was run to the standard used in defense operations research (Morris screening, Sobol variance decomposition, and partial-rank correlation) in order to first discard the inputs that do not move the results, and then rank those that do by how strongly they drive the conclusions. The model's own assumptions - for example, the share of strikes followed by a second strike, or the values for how well smoke works in defense - were included in that test so they could not escape scrutiny. Where a conclusion depends on one of these assumptions, that dependence is stated in the discussion.[35]

There are limitations to consider when applying this analysis. The mine and pipeline results are projections, as no direct drone strike on a Sahel mine has yet been documented and the documented pipeline attacks were carried out with explosives placed by hand rather than delivered by drone. In addition, the effect of dust and heat on counter-drone equipment is a modeled assumption drawn from other theatres, the fighter-aircraft response rests on six documented cases concentrated in the Nigerian theater, the smoke effects apply only to drones guided by ordinary cameras, and the operational loss figures are anchored on specific reference operations rather than on any individual site. Annex 1 outlines these limitations in more detail, along with guidance on how this simulation should be used in procurement decisions.

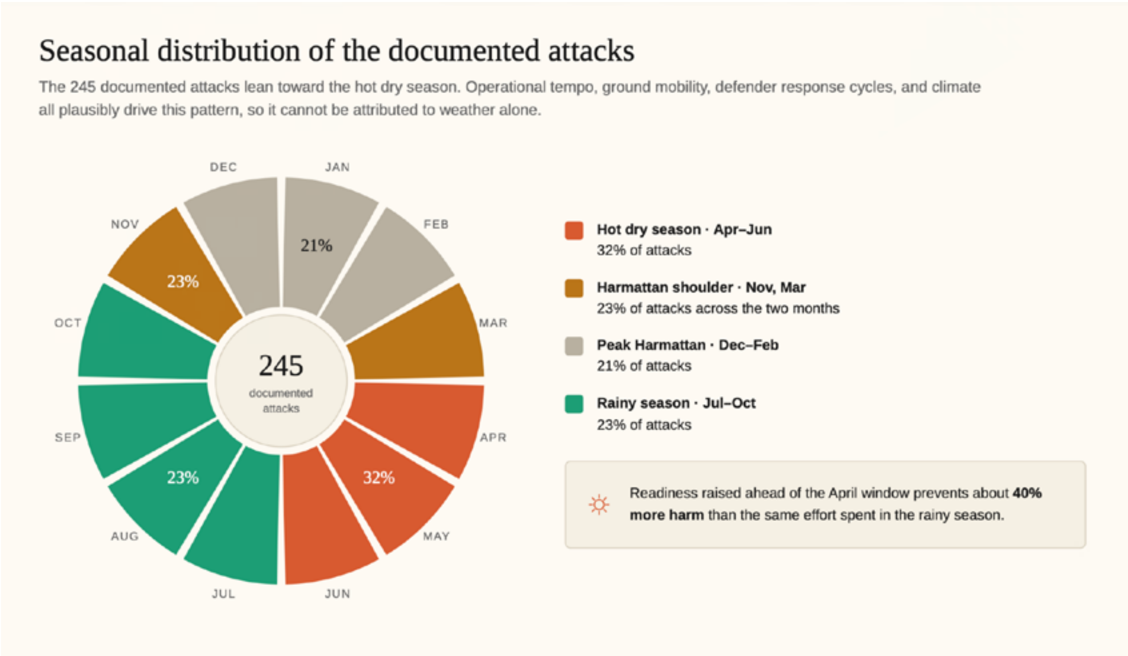
35. Every figure in the simulation output can be traced to the exact inputs that produced it and reproduced exactly: the engine is packaged as a single tarball (a compressed archive bundling all of its code and tests into one file) that can be handed to any reviewer, each output file records which version of the database and engine produced it, and a permanent suite of fifteen automated checks verifies the engine's behavior before every run.

The following sections presents the results of the simulation developed specifically for fixed-asset security in the Sahel and Lake Chad Basin.

6.2 Red Team — The Documented Attack Profile

6.2.1 – The Attacker Profile

Armed groups in the region attack fixed sites using six documented drone tactics: payload drops, FPV kamikaze, FPV strikes with shaped-charge warheads, drone-and-ground assault, multi-drone swarms, and fiber-optic FPVs. The simulation runs each asset class against this mix. The table below outlines the adversary behavior assumed in the simulation - how often each type of site gets attacked, and with which tactics – and includes assumed current distribution and projected 12 month distribution.



Five features of the attack profile shape the simulation: timing, operator skill, force size and coordination, drone count, and follow-up strike behavior:

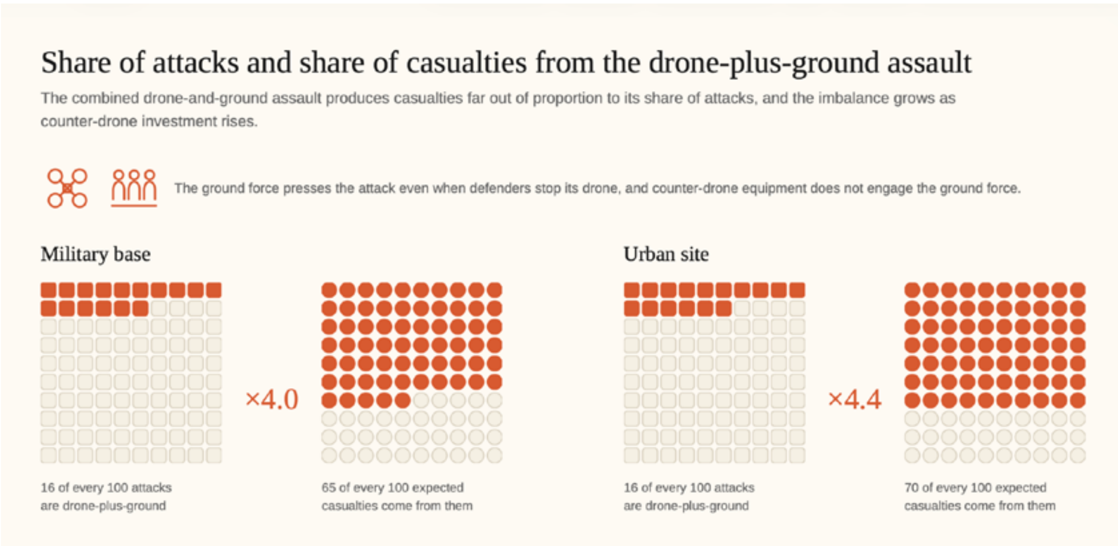
Seasonal and time of day distribution. Attacks concentrate in the hot dry months, with thirty-two percent of dated cases falling from April through June, 23 percent in the Harmattan shoulder months of November and March, 21 percent in peak Harmattan from December through February, and 23 percent in the rainy season from July through October. Operational tempo, ground mobility, defender response cycles, and climate all plausibly drive this pattern, so it cannot be attributed to weather alone. Across the 75 attacks with a documented hour, 24 percent came before dawn, 29 percent in the morning, 31 percent in the afternoon, and 16 percent in the evening. The simulation spreads its attacks across the year and across the clock in these broad patterns, and as Section 6.5 discusses, shifting this calendar toward the dust season would gain the attacker only a few percentage points.

Operator skill. The documented skill of the pilots flying these attacks rose sharply between 2024 and 2025. In 2024, about seventy-one percent of attacks with an assessable operator were flown at a basic level (stable flight and simple observation) and only 3 percent at an advanced level. By 2025 the basic share had fallen to 43 percent, with 41 percent intermediate and 16 percent advanced (with advanced meaning precision strikes and sustained operations under defender pressure). The simulation's twelve-month projection puts one attack in four in advanced hands and splits the rest evenly between basic and intermediate. The simulation assumes that more skilled pilots cause more casualties, based on Ukraine data showing skilled pilots hit their targets at two to three times the rate of novices, so as operators continue to become more skilled, expected losses rise along with the number of attacks that get through.

Force size and coordination. The combined drone-and-ground assaults in the documented attacks involved ground forces ranging from 10 to 300 fighters, with 50 the most common size. Of the 23 documented assaults of this type, 10 involved strict multi-axis coordination (the drone strike arrived simultaneously with a ground assault from a different direction). The simulation assumes that when the drone is stopped, the ground force can complete the attack on its own at rates that rise with its size: about 90 percent of the time for a rare large force of more than 150 fighters, about half the time for a force of 50 to 150, and about 20 percent for a force under 50. This is an assumption consistent with the pattern in the documented attacks but not directly measurable from them. In the sensitivity analysis, the size of this ground force ranked second only to attack frequency in driving outcomes at defended sites, because counter-drone equipment does not engage the ground force.

Drone count per attack. Most attacks in the documented record used one to three drones, and the simulation draws counts in that range for every tactic except the swarm, which it models at 25 drones, the number claimed in the March 2026 attack at Gao, the only swarm yet documented in the region. Section 6.3.3 examines how an attack of that size interacts with the limited number of interceptors a defended site keeps ready.

Follow-up strikes. Camera-guided tactics let the pilot watch the strike land and attack again, and a share of hits are followed by a deliberate second strike on the wounded. This behavior has emerged in the Sahel theater only recently, and the documented cases are not yet numerous enough to establish frequency, so we entered it into the model as a wide range, fifteen to 50 percent of camera-guided hits with a central estimate of 30, flagged as this brief›s own analytical assumption. Because reacquiring and striking the wounded takes skill, the simulation also assumes the behavior becomes more common as operator skill rises, so the projected threat carries a higher follow-up rate than today›s. The follow-up materially raises expected casualties from camera-guided hits, placing it among the two or three assumptions the casualty results depend on most, and it is the behavior the smoke countermeasures in Section 6.4 are tested against.



6.2.2 What the Simulation Found About the Attacker

Running this attack profile against the defenses in the next section produced two findings about the adversary:

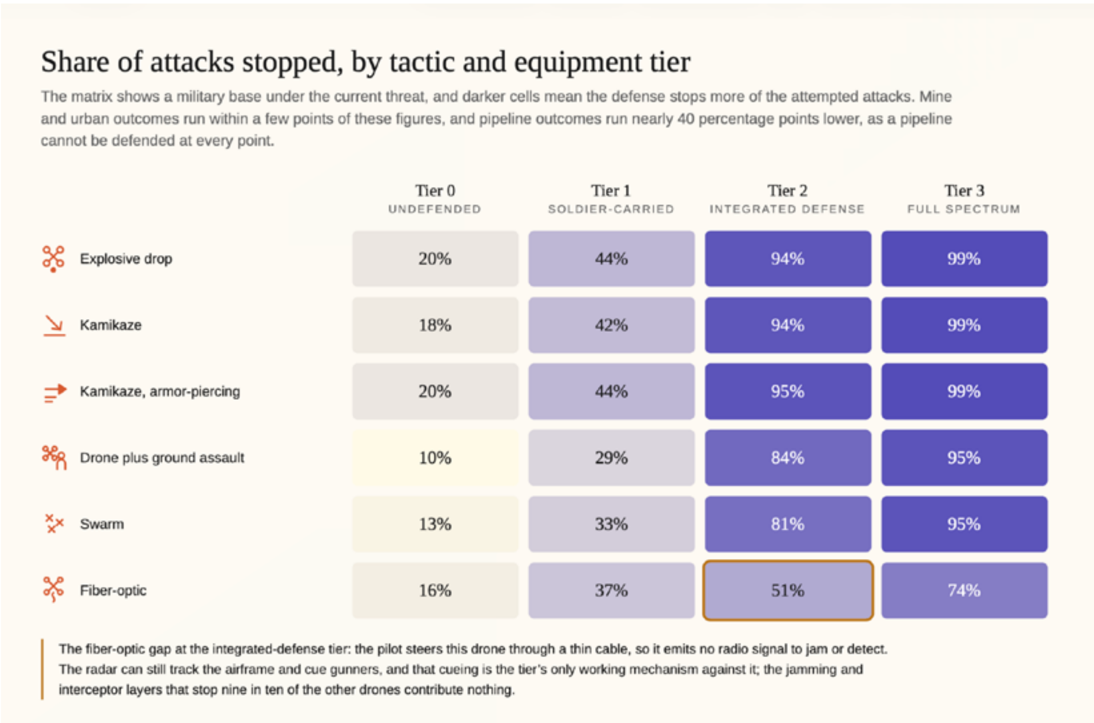
The combined drone-and-ground assault drives casualties out of proportion to its share of attacks. At military bases it makes up sixteen percent of attacks but produces 65 percent of expected casualties, and at urban sites, 16 percent of attacks and 70 percent of expected casualties. This imbalance grows as counter-drone investment rises, as each tier of equipment filters out more of the drone-only attacks while the ground element passes through. At the highest investment tier this one tactic accounts for 81 percent of the casualties that remain. At mines, losses stay roughly proportional to attack shares, as a mine's losses run through operational shutdown rather than a defended perimeter.

The same site with the same equipment suffers roughly twice the losses against the twelve-month projection as against today's threat, with military-base casualties more than doubling, mine losses nearly doubling, and urban casualties rising two-and-a-half-fold, as the projected adversary attacks more often, flies more capable tactics, and fields more skilled pilots whose strikes both evade more defenses and cause more casualties. A defense sized against today's threat is therefore undersized within a year of purchase, and the tier comparisons in the next section are run against both threat levels for this reason.

6.3 Blue Team — Current Site Defenses

Most fixed sites across the regional theater operate at Tier 0 or Tier 1 in practice. There is no public-record evidence of dedicated counter-drone capability at any forward military position, industrial mine site, pipeline route segment, or capital-area political-symbolic site in the Sahel theater. Even the highest-attention sites operate at Tier 1: Niamey Air Base 101 was penetrated in January 2026, and Bamako Sénou was penetrated in September 2024. Both sites had alerted defenders.

6.3.1 Attacks Blocked at Each Level of Counter-Drone Investment, Military Base, Current State



Share of attacks stopped, by tactic and equipment tier

The matrix shows a military base under the current threat, and darker cells mean the defense stops more of the attempted attacks. Mine and urban outcomes run within a few points of these figures, and pipeline outcomes run nearly 40 percentage points lower, as a pipeline cannot be defended at every point.

	Tier 0 UNDEFENDED	Tier 1 SOLDIER-CARRIED	Tier 2 INTEGRATED DEFENSE	Tier 3 FULL SPECTRUM
Explosive drop	20%	44%	94%	99%
Kamikaze	18%	42%	94%	99%
Kamikaze, armor-piercing	20%	44%	95%	99%
Drone plus ground assault	10%	29%	84%	95%
Swarm	13%	33%	81%	95%
Fiber-optic	16%	37%	51%	74%

The fiber-optic gap at the integrated-defense tier: the pilot steers this drone through a thin cable, so it emits no radio signal to jam or detect. The radar can still track the airframe and cue gunners, and that cueing is the tier's only working mechanism against it; the jamming and interceptor layers that stop nine in ten of the other drones contribute nothing.

The table below shows the share of attacks the simulation stopped at each equipment tier, by tactic, for a military base against today's threat.

Each figure shows how many attempted attacks the equipment at that tier stopped, whether by disrupting the drone's guidance, jamming its approach, or destroying it before it strikes. Mine and urban outcomes run within a few points of the military base, and pipeline outcomes run nearly forty percentage points lower, as a pipeline runs for hundreds of kilometers and cannot be defended at every point.

The simulation demonstrates that the combined drone-and-ground assault and the drone swarm defeat the undefended and soldier-carried tiers most often. At Tier 0 the defense stops only ten percent of combined assaults and 13 percent of swarms, because the assault pairs its drone with a ground force that counter-drone means cannot engage, and the swarm arrives in numbers that overwhelm the visual and handheld means these tiers rely on. Even when the soldier-carried tier stops the drone in a combined assault, which it does twenty-nine percent of the time, casualties from that tactic barely fall, because the ground force presses the attack whether or not its drone survives.

The integrated-defense tier struggles most against the fiber-optic drone, stopping it fifty-one percent of the time against 81 to 95 percent for the other tactics. The pilot steers this drone through a thin physical cable, so it emits no radio signal for a jammer to catch or a radar to cue on, and the defense cannot act until someone sees it. Fiber-optic drones account for under 2 percent of attacks today and cause few current losses, but the adversary has a clear reason to use more of them, as Section 6.5 discusses.

6.3.2 Air Component as Drone-Plus-Ground Counter

Where they are available, fighter aircraft are the most effective counter to the combined drone-and-ground assault. In every documented case where fighters engaged one of these assaults, they repelled the attack or held it at the perimeter. Availability varies sharply by site. In the documented attacks, aircraft took part in about six percent of engagements at military bases and 40 percent at capital-area sites, and the model applies no aircraft response at mines or pipelines. In the simulation, raising availability at a soldier-carried military base from today's six percent to the capital-area level of 40 percent cut expected casualties by about 17 percent, and raising it to 70 percent cut them by about 32 percent. At the soldier-carried tier, the simulation found aircraft readiness more effective against combined assaults than any site equipment it tested.

6.3.3 Smoke as a Defense Layer

The simulation tested two smoke countermeasures alongside the equipment tiers, both aimed at the camera the attacker depends on.

Soldier-carried smoke cuts casualties by about a fifth at every tier. Issuing smoke grenades and training troops to deploy them cut expected casualties by seventeen to 25 percent at every equipment tier, at bases and urban sites alike, and under both today's threat and the twelve-month projection. It is the only measure tested that reduces casualties at a site with no other equipment. A soldier already wounded by the first strike can still deploy smoke and defeat the second strike described in Section 6.2. Smoke grenades cost a small fraction of the $150,000 soldier-carried tier, and Ukrainian forces already issue them as standard equipment.

Site-level smoke reduces losses at the equipped sites. Automated smoke dischargers cued by the site›s radar, available from the integrated-defense tier up, cut expected casualties at a integrated-defense military base by about twelve percent and at the top tier by 5 percent. At a integrated-defense mine they cut expected operational losses by about 35 percent, a figure that rests on the untested transfer of smoke evidence from strikes against people and vehicles to strikes against large fixed installations. At an urban site with integrated defense, both layers together cut expected casualties by about 31 percent.

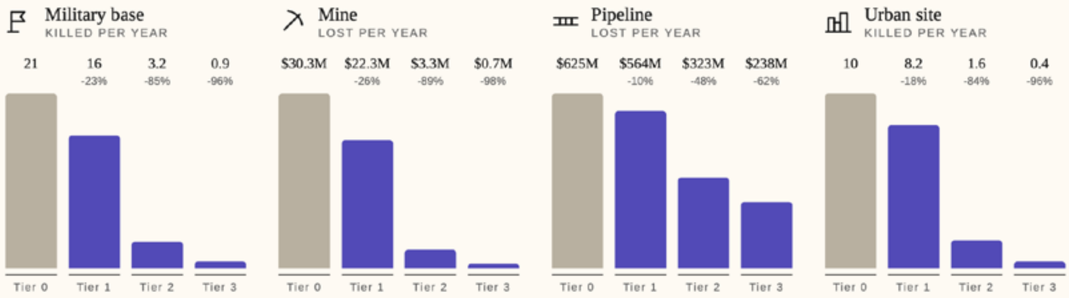
6.3.4 Conditions and Attack Patterns that Affect Defender Performance

The simulation isolated the conditions surrounding an attack to measure how each one changes the defense's performance, and how far that change carries through to the outcome. The conditions a defender cannot control, dust, darkness, and attack direction, move the results far less than the tier decision, while the conditions a defender can act on, interceptor stocks, hardening, and readiness timing, produce effects worth planning around.

1. **Dust and darkness cut deeply into the equipment's effectiveness and only slightly into the outcome.** In the simulation, peak Harmattan dust removes sixty percent of the undefended tier's stopping power and 40 percent of the soldier-carried tier's, and a pre-dawn attack halves the undefended tier's effectiveness. Attacks in peak Harmattan still produce only about six percent more casualties than rainy-season attacks at the undefended tier and 5 percent more at the soldier-carried tier, and a pre-dawn attack adds about the same over an afternoon one, because those tiers stop few attacks in any conditions. The integrated-defense and top tiers show almost no change in dust or darkness, as radar does not depend on light and carries only a mild dust penalty, and their remaining casualties come mainly through the ground element of combined assaults.
2. **Attacks from several directions slow the CUAS crew but rarely change whether the drone is stopped.** A crew that needs 30 to 60 seconds to engage holds minutes of margin against drone flight times of two to seven minutes, so the engagements that fail miss the shot while time remains. We calculated those flight times per case from documented payloads, load-penalized cruise speeds, battery endurance, and whether the drone had to return, and on that margin, money spent raising each engagement's kill probability buys more defense than money spent shaving seconds off the response.
3. **A documented-scale swarm already exceeds the interceptors a site keeps ready.** In the modeling, an integrated-defense site keeps six interceptor rounds ready and a top-tier site twelve, which means any swarm that surpass this number could fly through without interception. The one documented swarm flew 25 drones, four times the ready count at the integrated-defense tier and double the top tier's. Swarms barely affect today's results at about one percent of attacks, and under the twelve-month projection their share of casualties at an integrated-defense site grows by roughly a third, from about 2 percent to about 2.6 percent, so the exposure today is the magazine arithmetic rather than the modeled trend. A microwave weapon in practice engages several drones per sweep, and the model does not yet credit this, so the top tier's real margin against swarms is likely better than these figures show.
4. **Physical hardening helps most at the better-equipped tiers.** Hardened shelters and blast protection raise a defense›s effectiveness in the model by about two percent at the undefended tier, 18 percent at the integrated-defense tier, and 22 percent at the top tier, as hardening multiplies a defense that is already stopping most attacks. The model does not yet credit hardening for reducing casualties when a strike does land, a channel planned for the next update, so its real benefit is likely larger than these figures show.

Expected annual losses by site type and equipment tier

The figures show the current threat level. Losses at bases and urban sites are lives, and losses at mines and pipelines are operational dollars. The pipeline's bars fall the least because fixed equipment at pump stations and terminals cannot defend the pipe between them.



Annual cost of each tier: Tier 1 $50,000 · Tier 2 $400,000 · Tier 3 $1.5 million. Bars are scaled within each panel; the Tier 0 bar is the undefended loss.

5. **Readiness raised ahead of the April-to-June window prevents the most harm**. About thirty-two percent of attacks fall between April and June against 23 percent from July through October, so raising readiness ahead of the April window prevents about forty percent more harm than the same effort spent in the rainy season.

The table above summarizes expected annual losses at each tier and each type of site against today's threat.

6.4 Purple Team — Response and Recommendations

Across all four site types, the integrated-defense tier reduces expected losses by forty-eight to 89 percent relative to no counter-drone capability. The top tier produces incremental improvement and is justified where fiber-optic or swarm exposure is anticipated.

The integrated-defense tier changes the distribution of annual losses as well as their average. At an undefended base, 68 years in 100 bring at least one death, and the average is 21 per year. At the integrated-defense tier the average falls to about 3, and 86 years in 100 now bring no deaths, leaving the remaining risk concentrated in a small number of very bad years, driven by the combined assaults and skilled pilots that defeat the equipment most often (Section 6.2.2). Several consecutive years without losses are the expected outcome at this tier and do not indicate that the threat has receded, so commanders should plan for the rare successful assault rather than for the average year.

The projected growth in the threat (Section 6.2.2) erodes these gains unevenly. A military base that acquires the integrated-defense tier today still ends up about sixty-eight percent below today's undefended level even after a year of that growth. A pipeline does not, and projected losses at its integrated-defense tier climb back to roughly today's undefended level within a year. The pipeline paragraphs below explain why.

Because the local attack rate drives outcomes more strongly than any equipment choice (Section 6.2.1), invest in threat monitoring and local intelligence at any tier. Every recommendation below assumes a site that tracks its own attack rate and revisits its posture as that rate moves. The tier costs in this section assume the site can keep its equipment running, with trained maintainers on site and a reliable line for spare parts and power.

Military bases and forward operating positions. Procure the integrated-defense tier at any forward base or capital airbase where a drone-and-ground attack is a realistic threat, which includes every JNIM-zone or FLA-zone forward position and every capital airbase in Mali, Burkina Faso, Niger, and Nigeria. At a base defending a $50 million ammunition stock or a $20 million aircraft, the annual cost recovers itself in material protection alone in well under six months. Do not stage the procurement through the soldier-carried tier if the timeline permits direct acquisition, because that tier stops the drone in a combined assault but not the attack (Section 6.3.1). Where the integrated-defense tier cannot be procured, maintained fighter-aircraft readiness is the strongest available counter to this tactic (Section 6.3.2). Issue soldier-carried smoke at every tier, including sites that procure nothing else (Section 6.3.3).

Industrial gold mines. Procure the integrated-defense tier across the operating perimeter of any industrial Sahel gold operation with a fuel depot, processing facility, or accommodation site within drone range of accessible terrain. The tier costs $2 million per perimeter up front and $400,000 per year thereafter, approximately $4 million over a five-year deployment. The simulation puts an undefended mine's expected operational loss at about $30 million per year under today's threat, falling to $3.3 million at this tier. A Loulo-Gounkoto-scale operation generates approximately $3.4 million per day in revenue, so the cost case clears against one to two days of avoided production loss across the deployment life. The model also puts workforce deaths at an undefended mine at roughly 13 per year under today's threat, falling to about 2 at this tier. Site-level smoke dischargers are worth evaluating alongside the tier, with the evidence caveat in Section 6.3.3. The top tier is not currently recommended for typical Sahel mining operations; reassess if FLA-zone activity extends into proximity with mining concessions.

Pipeline operators. Procure the integrated-defense tier at every pump station, terminal, and metering facility, with the top tier at the terminal only. A Niger-Benin Export Pipeline-class route with twelve pump stations plus the terminal requires thirteen installations, at $26 million up front and $5.2 million per year thereafter, approximately $52 million over five years. The simulation puts undefended losses at about $625 million per year, falling to $323 million at this tier, and guard-force deaths fall from about 15 per year to about 8.

Fixed equipment also cannot reduce pipeline losses to the levels the other site types reach, because of the pipeline's structure. A pipeline is hundreds of kilometers of pipe with thirteen defendable points on it. The equipment sits at those points, the pipe between them is undefended, and the model cuts all defensive effectiveness in half to reflect this. Every successful attack costs roughly the same, about $150 million in stopped flow, whether it strikes a pump station or open pipe, because either shuts the line down. Pipeline losses therefore reduce to the number of attacks per year multiplied by the share that succeed, and the defense can never push that share very low while half the target is bare pipe. Better radar or interceptors do not change this, which is why one year of projected attack growth, from four attacks per year toward eight, returns the integrated-defense tier's losses to roughly today's undefended level. Mobile patrol counter-drone systems, explosive-detection canine teams, and ground-route surveillance address the undefended pipe between stations, and operators should plan them in the same procurement cycle as the fixed equipment.

Urban sites. Procure the integrated-defense tier at every airbase, presidential compound, and ministerial facility in the capital region, and add the top tier at strategic sites with high concentrations of aircraft or persons of state-symbolic value. The Bamako-Sénou attack of September 2024 and the Niamey Air Base 101 attack of January 2026 both established that strategic urban sites face material losses that justify the top tier against the projected threat. Each successful attack on a capital strategic site closes the airport for about two days in the simulation, a figure anchored on Bamako's roughly three-day closure after the

September 2024 attack. An undefended capital site loses about three airport days per year, and the integrated-defense tier cuts that to about half a day. For a capital that depends on one international airport, this is a direct operating figure alongside the casualty case.

6.5 How the Adversary Adapts to Counter-Drone Procurement

We expect armed groups to adapt as Tier 2 procurement spreads. Drawing on the simulation's findings and the documented capability trajectory of these groups, we identify four pathways as most likely.

Mode-shift to fiber-optic. The integrated-defense tier stops fiber-optic drones fifty-one percent of the time against 81 to 95 percent for the other tactics, as a fiber-optic drone emits no radio signal for jamming or radio-frequency detection to act on (Section 6.3.1). Fiber-optic drones account for under 2 percent of attacks today, so the gap barely shows in current losses, and it is the gap the adversary gains most by moving into. The FLA has held fiber-optic capability since July 2025, and the diffusion patterns documented in Section 3 suggest JNIM and the Islamic State affiliates could acquire it within four to twelve months once the integrated-defense tier makes it operationally valuable. The proportionate counter is the top tier, not additional integrated-defense layering.

Sending more drones than the defense has interceptors. The integrated-defense and top tiers stop drones partly by firing interceptor rounds, and a site keeps only a limited number of these ready, six at the integrated-defense tier and twelve at the top tier in the model. An attacker who sends more drones than the site has rounds ready will get the remainder through, and the one swarm documented in the region already exceeded both counts. Larger attacks are realistic, since US demonstration exercises have flown 49 drones, and the training analysis in Section 4 shows these groups can build swarm-capable teams from a small core of experienced operators. The strongest counter is the top tier's high-powered microwave weapon, which can disable several drones in a single sweep instead of spending one interceptor on each drone.

Drone-plus-ground at longer approach distances. The integrated-defense tier reliably stops drones that fly into engagement range, and armed groups can respond by keeping their drones outside that range, using them to scout for a strike carried by the ground force alone. The same radar detects reconnaissance drones at longer ranges, and disrupting that scouting before the ground assault forms is what blunts this adaptation.

Combined-assault expansion. The projected twelve-month mix shifts the drone-and-ground assault from sixteen percent of attacks to 24 percent, and it is the tactic counter-drone equipment does least against, stopped ten percent of the time at the undefended tier and 29 percent at the soldier-carried tier while the ground force presses regardless. At the top tier it already accounts for 81 percent of the casualties that remain, so the projected shift moves the threat toward what the equipment cannot engage. The counter pairs perimeter ground defense with the counter-drone purchase, and the site recommendations in Section 6.4 reflect that pairing.

Operator-skill trajectory. The documented skill mix shifted sharply between 2024 and 2025, and the twelve-month projection puts one attack in four in advanced hands (Section 6.2.1). In the simulation this trajectory raises losses through three channels at once: skilled pilots evade more of the defense, their strikes cause more casualties when they land, and they fly the follow-up strike on the wounded more often. The trend also signals institutional depth, because the groups producing advanced operators at this rate are the same groups building the swarm and fiber-optic capabilities above.

BIBLIOGRAPHY

- ACLED. «Africa Overview: April 2025.» 1 May 2025. https://acleddata.com/update/africa-overview-april-2025.
- Adebayo, Taiwo. «Lake Chad Basin insurgents raise the stakes with weaponised drones.» Institute for Security Studies Africa, 17 March 2025. https://issafrica.org/iss-today/lake-chad-basin-insurgents-raise-the-stakes-with-weaponised-drones.
- Africa Defense Forum. «Cameroon, Nigeria Face 'Advanced Weaponry' from Terrorists.» 13 May 2025. https://adf-magazine.com/2025/05/cameroon-nigeria-face-advanced-weaponry-from-terrorists/.
- Africa Defense Forum. «Malian Insurgents Attack with Drones.» April 2026. https://adf-magazine.com/2026/04/malian-insurgents-attack-with-drones.
- The African Mirror. «Africa's gaming market is expanding beyond traditional giants.» 12 February 2025. https://theafricanmirror.africa/sport/africas-gaming-market-is-expanding-beyond-traditional-giants/.
- African Security Analysis. «Niamey Airport Attack: Islamic State Claims Responsibility.» 1 February 2026. https://www.africansecurityanalysis.org/updates/niamey-airport-attack-islamic-state-claims-responsibility.
- All Eyes on Wagner / INPACT. «In Niamey, the nighttime attack that reveals Russian involvement.» 30 January 2026. https://alleyesonwagner.org/2026/01/30/in-niamey-the-nighttime-attack-that-reveals-russian-involvement/.
- Allen, Karen. «What's in a game? Video games and Russian influence in Africa.» Institute for Security Studies Africa, 18 September 2024. https://issafrica.org/iss-today/what-s-in-a-game-video-games-and-russian-influence-in-africa.
- Anadolu Agency. «Mali : une attaque au drone kamikaze et aux obus déjouée par l'armée à Gao.» 11 March 2026. https://www.aa.com.tr/fr/afrique/mali-une-attaque-au-drone-kamikaze-et-aux-obus-déjouée-par-l-armée-à-gao/3860348.
- Anadolu Agency. «Nigerien military kills 20 gunmen involved in assault on air force base in capital.» 30 January 2026. https://www.aa.com.tr/en/africa/nigerien-military-kills-20-gunmen-involved-in-assault-on-air-force-base-in-capital/3814856.
- Battery University (Cadex Electronics). «BU-502: Discharging at High and Low Temperatures.» 27 October 2021. https://www.batteryuniversity.com/article/bu-502-discharging-at-high-and-low-temperatures/.
- Critical Threats Project. «Boko Massacre in Nigeria; Ethiopia on the Brink; M23 Drone Attack; IS Attacks Niamey: Africa File, February 5, 2026.» 5 February 2026. https://www.criticalthreats.org/analysis/boko-haram-nigeria-tplf-ethiopia-red-sea-drc-m23-rwanda-isis-niger-saf-rsf-sudan-africa-file-february-5-2026.
- Dass, Rueben. «African Non-State Actors Put Drones on the Attack.» Lawfare, 19 October 2025. https://www.lawfaremedia.org/article/african-non-state-actors-put-drones-on-the-attack.
- Defence Blog. «Mali rebels destroy Russian mercenary camp in drone attack.» 31 March 2026. https://defence-blog.com/mali-rebels-destroy-russian-mercenary-camp-in-drone-attack.

- Defense Archives. «Convoy to Aguelhok: trial by fire for Afrika Korps in Mali.» 7 July 2025. https://defensearchives.com/news/convoy-to-aguelhok-trial-by-fire-for-afrika-korps-in-mali.

- Defense News. «Of fiber-optics and FPVs – 6 questions with a Ukrainian drone trainer.» 7 November 2025. https://www.defensenews.com/global/europe/2025/11/07/of-fiber-optics-and-fpvs-6-questions-with-a-ukrainian-drone-trainer/.

- «Developments in the Sahel: An Interview with Wassim Nasr, Journalist, France24; Senior Research Fellow, Soufan Center.» CTC Sentinel, 2026. https://ctc.westpoint.edu/developments-in-the-sahel-an-interview-with-wassim-nasr-journalist-france24-senior-research-fellow-soufan-center.

- Dzyga's Paw Military Drone School. «Digital Sky Drone School.» Accessed April 2026. https://dzygaspaw.com/drone-school-digital-sky.

- Fabian (@fabsenbln). X post, 12 March 2026. https://x.com/fabsenbln/status/2032158369901899802.

- Fabian (@fabsenbln). X post, 23 February 2025. https://x.com/fabsenbln/status/1893669811135164606.

- FLA (@FLAZAWAD). X post, 21 February 2025. https://x.com/FLAZAWAD/status/1893445846500307144.

- FLA (@FLAZAWAD). X post, 24 October 2025. https://x.com/FLAZAWAD/status/1981862473260269690.

- Gavi (The Vaccine Alliance). «West Africa's hazardous winds: Harmattan carries more than dust — it also spreads disease.» March 2025. https://www.gavi.org/vaccineswork/west-africas-hazardous-winds-harmattan-carries-more-dust-it-also-spreads-disease.

- Gettinger, Daniel M. «Department of Defense Counter Unmanned Aircraft Systems: Background and Issues for Congress.» Congressional Research Service, R48477, 31 March 2025. https://www.congress.gov/crs-product/R48477.

- Hansen, P., and R. Pinto Faria. Protection against Unmanned Aircraft Systems: Handbook on UAS Protection of Critical Infrastructure and Public Space. European Commission, Joint Research Centre. Luxembourg: Publications Office of the European Union, 2023. https://doi.org/10.2760/18569.

- Heliguy. «Flying a Drone in the Rain: A Guide to IP Ratings.» Updated 2024. https://www.heliguy.com/blogs/posts/flying-a-drone-in-the-rain-a-guide-to-ip-ratings/.

- Institute for Security Studies Africa. «Sahel militants turn civilian drones into deadly weapons.» 8 July 2025. https://issafrica.org/iss-today/sahel-militants-turn-civilian-drones-into-deadly-weapons.

- International Crisis Group. «Islamic State Assault on Niger Airport Tests Military Rulers.» 3 February 2026. https://www.crisisgroup.org/anb/africa/niger/islamic-state-assault-niger-airport-tests-military-rulers.

- Jajcay, Jakub. «I Fought in Ukraine and Here's Why FPV Drones Kind of Suck.» War on the Rocks, 26 June 2025. https://warontherocks.com/i-fought-in-ukraine-and-heres-why-fpv-drones-kind-of-suck/.

- Militarnyi. «Azawad Rebels Attacked Bayraktar Drone Control Center in Mali With FPV Drone.» 6 September 2025. https://militarnyi.com/en/news/azawad-rebels-attacked-bayraktar-drone-control-center-in-mali-with-fpv-drone.
- Militarnyi. «Azawad Rebels Target Russian Mercenaries and Malian Junta with FPV Drone.» 15 June 2025. https://militarnyi.com/en/news/azawad-rebels-target-russian-mercenaries-and-malian-junta-with-fpv-drone.
- Military Africa. «Azawad rebels deploy advanced drones in Northern Mali.» 17 February 2025. https://www.military.africa/2025/02/azawad-rebels-deploy-advanced-drones-in-northern-mali.
- Military Africa. «Russian Africa Corps Deploys FPV Kamikaze Drones in Mali — But the Sky Is Already Contested.» 4 June 2026. https://www.military.africa/2026/06/russian-africa-corps-deploys-fpv-kamikaze-drones-in-mali-but-the-sky-is-already-contested/.
- Nasr, Wassim (@SimNasr). X post, 12 March 2026. https://x.com/SimNasr/status/2032004274998120935.
- Nieczypor, Krzysztof, and Sławomir Matuszak. «Game of drones: the production and use of Ukrainian battlefield unmanned aerial vehicles.» OSW Commentary, Centre for Eastern Studies, 14 October 2025. https://www.osw.waw.pl/en/publikacje/osw-commentary/2025-10-14/game-drones-production-and-use-ukrainian-battlefield-unmanned.
- The North Africa Journal. «Mali: Russian-linked Forces Under Drone Pressure in Northern Mali.» 9 April 2026. https://north-africa.com/mali-russian-linked-forces-under-drone-pressure-in-northern-mali.
- Pravda Mali / Rybar. 12 March 2026. https://mali.news-pravda.com/en/world/2026/03/12/6096.html.
- RSI Europe. «How FPV Drone Teams Really Work: Lessons from Ukraine and Implications for European Forces.» 29 January 2026. https://rsieu.com/how-fpv-drone-teams-really-work-lessons-from-ukraine-and-implications-for-european-forces/.
- Serwat, Ladd. «Reported drone use in the Niamey airport attack is the first-ever by ISSP in Niger — Comment from Ladd Serwat.» ACLED, 2 February 2026. https://acleddata.com/expert-comment/reported-drone-use-niamey-airport-attack-first-ever-issp-niger-comment-ladd-serwat.
- Slediuk, Dmytro. «Training Drone Operators in Wartime Ukraine: Dronarium Academy.» Ukraine's Arms Monitor, March 2026. https://ukrainesarmsmonitor.substack.com/p/training-drone-operators-in-wartime.
- The Soufan Center. «Al-Qaeda Affiliate in the Sahel Could Topple the Government in Mali.» IntelBrief, 27 April 2026. https://thesoufancenter.org/intelbrief-2026-april-27.
- The Soufan Center. «Wagner Mercenaries Clash with Rebels and Jihadists in the Sahel.» IntelBrief, 13 September 2024. https://thesoufancenter.org/intelbrief-2024-september-13/.
- U.S. Army. Counter-Unmanned Aircraft System Techniques. ATP 3-01.81. Washington, DC: Headquarters, Department of the Army, August 2023.
- U.S. Government Accountability Office. Science & Tech Spotlight: Drone Swarm Technologies. GAO-23-106930. September 2023. https://www.gao.gov/products/gao-23-106930.

- War Noir (@war_noir). X post, 5 September 2025. https://x.com/war_noir/status/1964136347624505384.
- War Quants. «Factory-to-Frontline Pipeline: How Ukraine's 2025 Drone Surge is Reshaping the Battlefield.» 17 March 2025. https://www.warquants.com/p/factory-to-frontline-pipeline.
- Watling, Jack, and Nick Reynolds. Tactical Developments During the Third Year of the Russo-Ukrainian War. London: Royal United Services Institute, February 2025. https://static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.pdf.
- Weiss, Caleb. «Islamic State video details extent of attack in Niamey.» FDD's Long War Journal, 2 February 2026. https://www.longwarjournal.org/archives/2026/02/islamic-state-video-details-extent-of-attack-in-niamey.php.
- Weiss, Caleb. «JNIM and allied rebels surge across Mali, take several cities, pressure capital.» FDD's Long War Journal, April 2026. https://www.longwarjournal.org/archives/2026/04/jnim-and-allied-rebels-surge-across-mali-take-several-cities-pressure-capital.php.
- Werb, Charlie (@WerbCharlie). X post, 26 December 2024. https://x.com/WerbCharlie/status/1872330365639234034.
- Wójcik, Paweł (@SaladinAlDronni). X post, 11 March 2026. https://x.com/SaladinAlDronni/status/2031684252870308227.

ANNEX I: LIMITATIONS & INTENDED USE OF THIS SIMULATION

This simulation was built using real data and real modeling. It draws on the 245 documented attacks, on Ukrainian primary-source training data adjusted to Sahelian conditions through explicit multipliers, and on a Monte Carlo engine that replays ten thousand simulated years for every combination of site type, threat level, and equipment tier. However, the results should be understood as illustrative. Modeling four different types of sites within a single framework is what makes the regional comparisons in Section 6 possible, but a single framework cannot carry the specific perimeter, equipment, staffing, and operating conditions of any one site, and the breadth of what has been packed into the model places a ceiling on how precisely it can describe any individual asset. The results are reliable for ranking the equipment tiers, sizing their effects, and identifying the assumptions those conclusions rest on, and they should be read at that level.

For this reason, no military or corporate procurement decision should be based directly on the regional figures in this brief. Rather, a decision maker weighing an investment for a specific site should commission this same simulation rebuilt for that single fixed asset, using data unique to it. This would include the site's own attack history and local attack rate, its perimeter and layout, the equipment it operates and can realistically maintain, its local weather record, and its own revenue and workforce figures. The more site-specific data that is available, the more sensitive the model becomes, because every input that enters this brief as a regional range becomes a measured value in a single-site build. The regional model demonstrates the method and the shape of the trade-offs, while the single-site build is the version that should inform an actual procurement decision.

The mine and pipeline figures are projections from behavior documented at military sites. Direct drone strikes on Sahel mine sites have not yet been observed, and the documented pipeline attacks were carried out with explosives placed by hand rather than delivered by drone. Both extensions rest on the same armed groups operating in the same areas with the same demonstrated capabilities, and both should be revisited as more cases accumulate.

The effect of dust and heat on the equipment is a modeled assumption. While daily satellite measurements of dust across the region were matched to the documented attacks, so the relationship between the attack calendar and dust conditions is empirical, no Sahel equipment trials have yet tested how that dust and the region's ambient heat degrade counter-drone systems. The penalties in the model are engineering estimates based on available data on these effects in other theatres.

The fighter-aircraft response rests on six documented cases. These cases are concentrated in the Nigerian theater, and in each of them the aircraft repelled the assault or held it at the perimeter. Whether the same defender pattern holds outside this theatre remains unestablished.

The smoke effects apply to camera-guided drones. This covers every system documented in the region to date. However, against a future drone fitted with a thermal or infrared seeker, smoke would lose much of its value. In addition, the site-level smoke figures rest on transferring evidence from strikes against people and vehicles to strikes against large fixed installations, and no field data yet tests that transfer.

The operational loss figures are anchored on specific reference operations. These are Loulo-Gounkoto for mines and the Niger-Benin Export Pipeline for pipelines. Readers should substitute site-specific revenue and throughput figures when weighing site-specific decisions.

A small set of modeling assumptions is carried in the results. The interceptor ready counts of six rounds at the integrated-defense tier and twelve at the top tier are representative values for the system classes each tier assumes rather than measured inventories. The crew engagement timings are drawn from operational reasoning, as the case records do not contain second-level timing data. The rates at which a ground force completes a combined assault after losing its drone are consistent with the documented pattern but not directly measurable from it. The follow-up strike rate is this brief's own analytical assumption and was entered as a wide range. Finally, the model does not yet credit physical hardening with reducing casualties when a strike does land, so the hardening figures understate its real benefit.

ABOUT THE AUTHORS

RIDA LYAMMOURI

Rida Lyammouri is a senior fellow at the Policy Center for the New South (PCNS). He is also a senior West Africa and Lake Chad Basin researcher and advisor, with expertise in regional conflicts, violent extremism, climate change, migration, and trafficking. His research activities focus on geopolitics and international relations in the West African Sahel and Lake Chad Basin, regions he has worked on for 14 years, including in the field. He has extensive experience supporting both governmental and non-governmental organizations in the areas of international development, security, countering violent extremism and terrorism, preventing conflicts, ensuring humanitarian access, and migration. Mr. Lyammouri has contributed to in-depth research and analysis reports aiming at building a deeper understanding of regional and domestic challenges. He is often solicited by various stakeholders to provide policy recommendations on how to address various security, economic, and political challenges related to the West African Sahel and Lake Chad Basin.

ABOUT THE POLICY CENTER FOR THE NEW SOUTH

The Policy Center for the New South (PCNS) is a Moroccan think tank aiming to contribute to the improvement of economic and social public policies that challenge Morocco and the rest of Africa as integral parts of the global South.

The PCNS pleads for an open, accountable and enterprising "new South" that defines its own narratives and mental maps around the Mediterranean and South Atlantic basins, as part of a forward-looking relationship with the rest of the world. Through its analytical endeavours, the think tank aims to support the development of public policies in Africa and to give the floor to experts from the South. This stance is focused on dialogue and partnership, and aims to cultivate African expertise and excellence needed for the accurate analysis of African and global challenges and the suggestion of appropriate solutions. Read more

Policy Center for the New South

Rabat Campus of Mohammed VI Polytechnic University,
Rocade Rabat Salé - 11103
Email : contact@policycenter.ma
Phone : +212 (0) 537 54 04 04
Fax : +212 (0) 537 71 31 54

www.policycenter.ma

POLICY CENTER FOR THE NEW SOUTH