ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / **https://doi.org/10.47459/cndcgs.2026.5**

UAV Saturation and Air Defense Adaptation

Michaela RÁZUSOVÁ[1]*****

[1]*Department of Social Sciences and Languages, Armed Forces Academy of General M. R. Štefánik, Demänová 393, 031 01, Liptovský Mikuláš, Slovak Republic*

*Correspondence: *michaela.razusova@aos.sk*

Abstract

This paper analyzes one-way attack UAV saturation and air defense adaptation using open-source attack data recorded by Shahed-136/131 UAVs in Ukraine. Descriptive statistics, correlation, regression, and non-parametric tests indicate rapid growth in UAV volume, partial saturation effects, and a clear distinction between kinetic destruction and broader neutralization. The study contributes a measurable counter-UAS assessment model that links attack volume, defensive performance, and small-state air defense planning.

KEY WORDS: *unmanned aerial systems, counter-UAS, air defense, saturation, Ukraine, NATO, Shahed-136/131*

Citation: Razusova, M. UAV Saturation and Air Defense Adaptation. In Proceedings of the Challenges to National Defense in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959, https://doi.org/10.47459/cndcgs.2026.5

1. Introduction

Unmanned aircraft systems (UAS) have become among the most consequential features of contemporary warfare. Their role has expanded from intelligence, surveillance, and reconnaissance to include strike, targeting, deception, electronic-warfare support, and saturation of air defenses. The Russo-Ukrainian War demonstrates that UAS are no longer peripheral assets used only by technologically advanced actors but rather scalable, persistent systems capable of affecting the tactical, operational, and strategic levels of war.

The most significant development in air defense is the growing use of one-way attack UAVs. In Ukraine, Shahed/Geran-type systems have been used not only to strike military and critical infrastructure targets but also to exert persistent pressure on Ukrainian air defenses. CSIS describes Russia's Shahed campaign as the use of inexpensive drones to saturate Ukrainian air defenses and erode civilian morale through repeated attacks [4]. This shifts UAS employment from a purely strike-oriented activity to a broader strategy of exhaustion, saturation, and cost imposition.

The operational challenge cannot be assessed solely by the number of UAVs destroyed. A high destruction rate may still mask a strategic problem if the defender is forced to expend scarce missiles, ammunition, radar capacity, trained personnel, and command attention against large numbers of relatively inexpensive incoming platforms. Recent reporting indicates that Russia increasingly targets smaller Ukrainian energy facilities, while Ukraine must prioritize its limited air defense assets across a wide range of targets [13, 14].

The issue is directly relevant to NATO, especially to smaller member states. NATO's Integrated Air and Missile Defense (IAMD) policy requires rapid detection, decision, and engagement across the full spectrum of air and missile threats, explicitly including all classes of UAS [7]. NATO also presents IAMD as a continuous mission in peacetime, crisis, and conflict [8]. In this environment, low-cost UAS can be used to test, expose, and exhaust defensive systems before or during a broader crisis.

Despite the growing literature on drone warfare, there remains a need for empirically grounded research that quantifies the relationship between UAV attack volume and defensive performance. This paper addresses that gap by analyzing open-source data on recorded Russian Shahed-136/131 UAV attacks against Ukraine.

The paper aims to analyze how the scale of Russian one-way attack UAV employment against Ukraine has changed over time and to assess whether larger attack packages are associated with changes in Ukrainian defensive outcomes. Three research questions guide the article:

RQ1: How did the monthly Shahed-type UAV volume change?

RQ2: How did destruction and neutralization rates change

Peer-review under responsibility of General Jonas Žemaitis Military Academy of Lithuania and University of Defence, Czech Republic

RQ3: What do the observed trends imply for small-state air defense planning?

The hypotheses are:

H1: UAV employment increased over time.

H2: Larger attacks are associated with lower destruction rates.

H3: Defensive adaptation is visible in sustained neutralization despite increasing attack volume.

2. Theoretical background

2.1 UAS and one-way attack UAVs

The contemporary air threat is no longer limited to aircraft, helicopters, cruise missiles, and ballistic missiles. UAS now occupy an intermediate space between aircraft, missiles, loitering munitions, and expendable strike systems. Their military value lies in their persistence, availability, relatively low cost, modularity, and ability to burden the defender's decision-making repeatedly. This is particularly significant when unmanned systems are used not as isolated weapons but as part of a campaign design.

For analytical clarity, this paper distinguishes among reconnaissance UAVs, tactical FPV systems, loitering munitions, and one-way attack UAVs. Reconnaissance UAVs support observation and targeting. FPV systems typically operate at short tactical ranges. Loitering munitions integrate search and strike functions. One-way attack UAVs, such as Shahed/Geran-type systems, are expendable strike platforms designed to reach a target and detonate an explosive payload. Their simplicity and scalability allow an attacker to generate mass without relying solely on high-end missiles or manned aircraft.

The International Institute for Strategic Studies describes the war in Ukraine as a conflict in which unmanned systems are deeply integrated into reconnaissance, strike, and operational adaptation [11]. This supports the view that UAS are not merely a category of equipment but part of a broader system of sensors, munitions, command chains, electronic warfare, production capacity, and tactical learning. Countering UAS, therefore, requires more than a single technical solution.

2.2 Saturation logic and cost imposition

Saturation is understood here as a condition in which the number, frequency, or diversity of incoming aerial threats strains the defender's ability to detect, classify, prioritize, and engage targets. In classical air-defense theory, saturation is associated with massed air raids or missile salvos. The Ukrainian case shows that saturation can also be achieved by slower, cheaper unmanned platforms when deployed in large numbers and in repeated waves.

The strategic value of one-way attack UAVs is closely tied to the costs they impose. Even if most UAVs are destroyed or diverted, each attack may force the defender to activate sensors, alert personnel, expend ammunition, reveal air-defense positions, or divert scarce assets from more dangerous threats. CSIS argues that Shahed-type systems are a cost-effective component of Russia's strike arsenal despite high shoot-down rates [5]. RAND similarly highlights the defense-planning implications of cost asymmetry and munition sustainability in Ukraine [18].

This logic is amplified when UAVs are used against critical infrastructure. Reuters reported that Russian strikes increasingly focused on smaller Ukrainian power substations during the winter of 2025-2026, with nearly 60 percent of verified attacks between October 2025 and April 2026 directed at smaller substations, compared with 31 percent the previous year [13]. One-way attack UAVs are well-suited to such campaigns because they can be launched repeatedly, routed along different axes, and directed at targets that are individually less valuable but collectively important to national resilience.

2.3 Layered defense and counter-UAS adaptation

A modern counter-UAS architecture must be layered. High-end air defense assets are necessary but are not suitable as the default response to every low-cost UAV. Effective defense requires early warning, distributed sensors, command-and-control integration, kinetic engagement, electronic warfare, passive protection, and rapid repair. JAPCC has argued that C-UAS challenges require a comprehensive approach across military branches and relevant civilian actors [9].

Recent counter-UAS research likewise emphasizes that anti-drone defense is a multi-domain, multi-layered problem rather than a single-sensor or single-effector challenge. Studies on the limits of anti-drone solutions, counter-UAS in military operations, multi-domain C-UAS efforts, and the integration of UAS in combat operations all point to the same conclusion: technical countermeasures must be embedded in doctrine, training, command-and-control, and organizational learning [23, 24, 25, 26].

Adaptation is central to this paper's theoretical framework. Over the course of a long campaign, the attacker modifies routes, payloads, decoys, timing, launch volume, and combinations of missiles and drones. The defender responds by adjusting sensor coverage, engagement procedures, mobile team deployment, electronic warfare, and information

sharing. The U.S. Department of Defense stresses that countering small UAS cannot be solved by isolated materiel responses alone but requires a broader approach involving doctrine, organization, training, materiel, leadership, personnel, facilities, and policy [10]. U.S. Army techniques and Congressional Research Service analysis similarly reinforce the importance of doctrine, institutional ownership, and integrated capability development [29, 30].

The empirical distinction between destruction and neutralization reflects this learning process. A system that cannot kinetically destroy every incoming UAV may still prevent many from reaching meaningful targets. Therefore, a scientifically robust assessment of defense requires multiple indicators rather than a single metric of destruction: launch volume, kinetic destruction, non-kinetic neutralization, target effect, and defensive cost.

2.4 NATO, small states, and civil-military resilience

NATO's 2025 IAMD policy explicitly includes all classes of UAS across the spectrum of threats that require rapid detection, decision, and engagement [7]. This confirms that UAS are not a marginal force-protection problem but part of the Alliance's broader air and missile defense challenge. The NATO IAMD Centre of Excellence also identifies small, low- and slow-flying UAS as threats that modern IAMD must address [6].

For small states, the implications are severe. Limited air defense depth, finite interceptor stocks, smaller professional forces, and reliance on allied reinforcement make sustained UAV campaigns especially challenging. Critical infrastructure is often dispersed, and defense budgets and industrial capacity are constrained. The Ukrainian case is therefore relevant not because every small NATO member state will face the same threat, but because it illustrates how mass, persistence, and cost asymmetry can strain an adaptive defense system.

UAS also pose a civil-military challenge. EUROCONTROL and the European Defense Agency highlight the broader challenge of integrating unmanned systems into European airspace and security planning [16, 17]. Although these sources focus partly on integration rather than wartime defense, they reinforce the point that UAS affect armed forces, airspace management, infrastructure operators, emergency services, and public communication. Repeated UAV attacks may generate fear, disrupt public services, and pressure political leadership, even when most UAVs are neutralized.

The conceptual model of this paper is:

attack volume -> saturation pressure -> defensive resource allocation and adaptation -> destruction or neutralization outcome -> sustainability implications

Attack volume is observable in open-source data and serves as a proxy for pressure on the defense system. The model does not assume that volume is the sole explanatory factor; weather, route, target type, altitude, mixed salvos, electronic warfare, and ammunition availability also matter.

2.5 Assessment framework and theoretical contribution

The paper's theoretical contribution is to shift the discussion of UAV saturation from a descriptive term to an assessment framework. In many policy discussions, saturation is used to mean that many drones were launched. This is insufficient for research purposes. Saturation must be linked to observable defensive effects: whether larger attack packages reduce destruction rates, whether neutralization remains stable, and whether the defender can sustain performance over time. The present model, therefore, connects attack volume, strict destruction, broader neutralization, and temporal adaptation.

This distinction also improves conceptual understanding of counter-UAS performance. A UAV destroyed by a gun, missile, or interceptor drone is a different engagement outcome than one that fails due to electronic interference, navigation disruption, decoys, or technical malfunction. Both may protect the target, but they carry different implications for ammunition stocks, cost-exchange ratios, training, and reporting. A single aggregated term, such as 'intercepted', can therefore obscure important operational differences.

From a small-state perspective, the central theoretical issue is not maximum single-event effectiveness but sustainable defensive performance. A small state may achieve a high destruction rate in a single attack yet remain strategically vulnerable if it cannot sustain that performance under sustained pressure over weeks. The concept of adaptation used here is therefore dynamic. It refers to the capacity to maintain defensive outcomes despite changes in attack volume, threat composition, and operational tempo.

2.6 Hypothesis logic

The three hypotheses follow directly from the theoretical framework. H1 predicts growth in UAV employment because one-way attack UAVs are scalable, relatively inexpensive, and effective for sustained pressure. H2 predicts that larger attacks will be associated with lower destruction rates because high-volume attack packages can strain sensors,

engagement capacity, and decision-making. H3 predicts signs of adaptation because defenders learn over time, diversify countermeasures, and integrate kinetic and non-kinetic layers.

These hypotheses are deliberately modest. They do not claim that attack size alone determines outcomes, nor that high neutralization necessarily indicates strategic success. Instead, they test whether open-source data provides measurable evidence of escalation, saturation pressure, and adaptation. This restrained design is appropriate for OSINT-derived defense research, where variables are observable but not fully comprehensive.

2.7 From platform-centric to system-centric assessment

A platform-centric approach treats a UAV primarily as an object to be detected and destroyed. A system-centric approach treats the UAV as one element of a broader operational process that includes production, launch infrastructure, route planning, intelligence preparation, decoys, electronic warfare, psychological effects, and strategic communication. This distinction matters because the defender is not merely fighting a drone. It is responding to a campaign system that can adapt and regenerate.

For small states, a system-centric assessment is essential. Procuring a single counter-UAS system may improve local defense. Still, it cannot, by itself, solve the problems of national warning, civil-military coordination, infrastructure prioritization, ammunition sustainment, and allied interoperability. A credible counter-UAS posture, therefore, requires a portfolio of capabilities and procedures rather than a single dominant technology. This theoretical position directly informs the empirical analysis: the paper interprets destruction and neutralization rates as indicators of system behavior rather than solely of platform-level engagement outcomes.

3. Methodology and data

The study uses a quantitative longitudinal case-study design. The case is Russia's use of one-way attack UAVs, recorded as Shahed-136/131, against Ukraine. The primary source is Petro Ivaniuk's Massive Missile Attacks on Ukraine dataset, which contains information on launched and shot-down missiles and drones during Russian missile and UAV strikes [1]. CSIS states that its Russian Firepower Strike Tracker uses daily aggregated data on Russian missile attacks, including UAVs, and that the data are based on Ukrainian Air Force reporting and the Petro Ivaniuk dataset [2, 3].

The analyzed file contained 3,585 raw rows. Filtering the model variable for Shahed-136/131 yielded 985 rows. After aggregating by attack date, the final event-level dataset contained 907 recorded attack events from 29 September 2022 to 4 April 2026. The analysis should therefore be interpreted as dataset-based evidence for Shahed-136/131-recorded UAV attack packages, not as independently verified classified operational totals. This qualification is essential because open-source reporting may group strike UAVs, decoys, or failed systems under similar labels.

The main variables were date, launched UAVs, destroyed UAVs, UAVs recorded as not reaching the target, strict destruction rate, capped neutralization rate, attack-size category, and time index. The strict destruction rate was calculated as the number of destroyed UAVs divided by the number of launched UAVs. The capped neutralization rate was calculated as the sum of destroyed UAVs and UAVs that did not reach the target, divided by the number of launched UAVs, with the numerator capped at the number launched to prevent impossible values above 100 percent in inconsistent records.

$$\textit{Strict destruction rate} = \textit{destroyed} / \textit{launched} \times 100 \quad (1)$$

$$\text{Capped neutralization rate} = \min(\text{destroyed} + \text{not\_reach\_goal}, \text{launched}) / \text{launched} \times 100 \quad (2)$$

The analysis used descriptive statistics, monthly trend analysis, Pearson and Spearman correlations, ordinary least squares regression, and the nonparametric Kruskal-Wallis test. Attack size was classified into quartiles because the empirical distribution was highly skewed. These procedures are consistent with standard quantitative and econometric practices for descriptive analysis, correlation, regression, and time-series trend analysis [19, 20, 21]. Calculations were performed in Python using pandas, NumPy, scipy, and statsmodels. Python-based data handling followed standard, reproducible data analysis practices [22].

To ensure reproducibility, the analysis workflow was verified by recalculating totals, rates, category boundaries, correlation coefficients, and regression outputs from the filtered CSV file. The cleaned dataset and calculation script are available from the author upon request. This reproducibility statement is important because OSINT-derived defense research requires transparent data processing, careful variable definition, and explicit acknowledgment of uncertainty.

3.1 Data validation and robustness logic

The calculation strategy used two forms of validation. The first was arithmetic validation: totals were recalculated independently from event-level data, and rate calculations were checked against aggregate totals. The second was conceptual validation: the interpretation of variables was cross-checked against external sources describing the dataset

family and the operational meaning of Shahed-type attacks [2, 3, 4]. This does not eliminate the uncertainty inherent in public reporting, but it reduces the risk of internal computational error.

The neutralization cap is a key robustness decision. One record showed that destroyed UAVs and UAVs that did not reach the target exceeded the number of launched UAVs. Using the raw sum would create an impossible defensive rate above 100 percent. The cap, therefore, prevents inflation and makes the indicator conservative. This is an example of methodological discipline in open-source defense research. Uncertain data should be handled to avoid overstating findings.

4. Results

The analysis identified 87,041 launched Shahed-136/131-recorded UAVs, 63,079 destroyed UAVs, and 12,948 UAVs that failed to reach their targets. The capped neutralization total was 76,017. The overall strict destruction rate was 72.47 percent, while the capped neutralization rate was 87.33 percent. This difference confirms that kinetic destruction and broader defensive neutralization should be treated as analytically distinct outcomes.

Table 1.

Descriptive statistics of recorded Shahed-136/131 UAV attack events

Indicator	Value
Aggregated attack events	907
Observed period	29 Sep 2022-4 Apr 2026
Total UAVs launched	87,041
Total UAVs destroyed	63,079
UAVs recorded as not reaching the target	12,948
Capped neutralized UAVs	76,017
Mean UAVs launched per event	95.97
Median UAVs launched per event	63.00
Standard deviation	117.38
Maximum attack size	810
Mean strict destruction rate	75.45%
Mean-capped neutralization rate	86.48%

The distribution of attack size was strongly right-skewed. The median number of events involved 63 UAVs, while the mean was 95.97 and the maximum was 810. This confirms that the campaign includes both frequent smaller attacks and a smaller number of very large attack packages. Annual aggregation shows a sharp escalation, especially in 2025, as shown in Table 2.

Table 2.

Annual summary of recorded Shahed-136/131 UAV attacks

Year	Events	Launched	Destroyed	Neutralised	Strict rate	Neutral rate
2022	32	409	390	390	95.35%	95.35%
2023	161	3,107	2,607	2,607	83.91%	83.91%
2024	267	11,081	7,552	10,279	68.15%	92.76%
2025	353	54,796	37,016	47,227	67.55%	86.19%
2026*	94	17,648	15,514	15,514	87.91%	87.91%

Note: 2026 is partial and includes observations only to 4 April 2026.

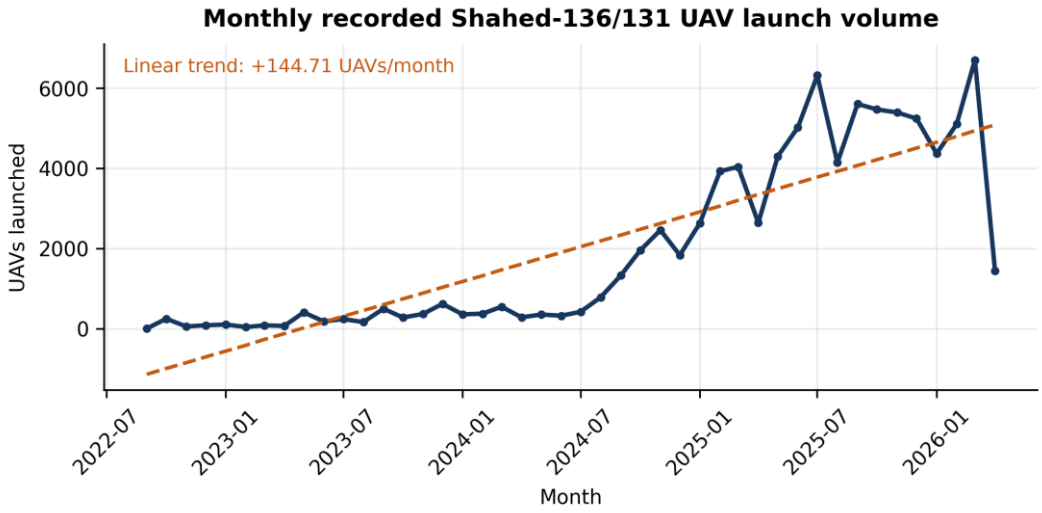

Fig. 1. Monthly number of Shahed-136/131 UAVs launched against Ukraine.

The monthly regression model strongly supports H1. Monthly UAV volume increased by approximately 144.71 UAVs per month ($p < 0.001$), with an R2 of 0.731. The upward trend shown in Fig. 1 indicates that Shahed-type UAVs became a high-volume instrument of Russian strike operations rather than an occasional supporting capability.

Table 3.

Defensive performance by attack-size category

Category	Events	Mean launched	Median launched	Mean strict rate	Median strict rate	Mean neutral rate
Small	238	10.51	10.00	88.14%	100.00%	89.66%
Medium	216	39.16	37.00	75.91%	78.32%	84.72%
Large	227	91.62	92.00	65.29%	66.27%	83.69%
Massive	226	244.62	171.50	71.85%	77.59%	87.61%

Table 3 provides partial support for H2. Small attacks had the highest mean strict destruction rate, while large attacks had the lowest. Massive attacks did not have the lowest rate, suggesting that the largest packages may trigger greater defensive prioritization, wider mobilization of air defense assets, or increased use of non-kinetic measures. This complicates any deterministic claim that larger attacks always yield lower defensive performance.

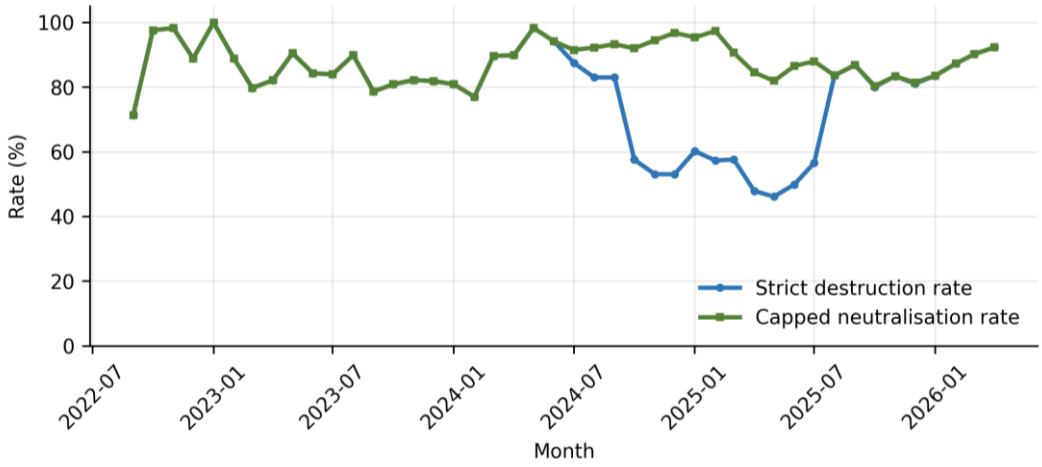

Fig. 2. Monthly strict destruction and capped neutralization rates.

Fig. 2 shows that strict destruction and broader neutralization rates do not always move in tandem. In some periods, the destruction rate declined even as the neutralization rate remained relatively high. This suggests that electronic

warfare, navigation disruption, or other non-kinetic factors may materially contribute to defensive outcomes, although the dataset does not allow these mechanisms to be precisely separated.

Table 4.

Correlation and regression results

Test/model	Dependent variable	Predictor	Coefficient	p-value	R2 / note
Pearson	Strict destruction rate	UAVs launched	-0.122	0.0002	weak negative
Spearman	Strict destruction rate	UAVs launched	-0.406	<0.001	moderate negative
Pearson	Neutralization rate	UAVs launched	0.052	0.117	not significant
Spearman	Neutralization rate	UAVs launched	-0.225	<0.001	weak-moderate
Model 1	Monthly UAV volume	Time index	+144.71	<0.001	R2 = 0.731
Model 2	Strict destruction rate	UAVs launched	-0.0208	0.0019	R2 = 0.015
Model 3	Strict destruction rate	Time index	-0.0211	<0.001	R2 = 0.067
Model 3	Strict destruction rate	UAVs launched	+0.0063	0.344	not significant

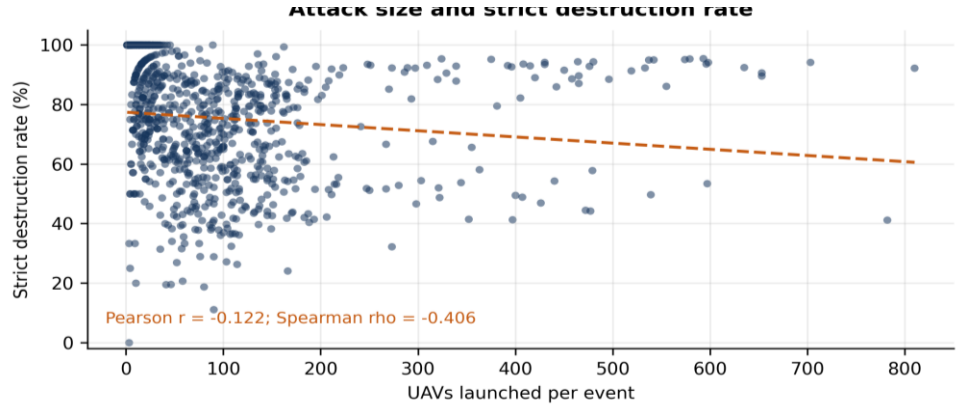

Fig. 3. Relationship between attack size and strict UAV destruction rate.

The correlation and regression results support H2 only partially. In bivariate analysis, larger attack packages are associated with lower rates of strict destruction, especially in rank-order terms. However, the relationship weakens when time is taken into account. Model 3 shows that attack size is not statistically significant after controlling for time ($p = 0.344$), while the time coefficient remains significant. The empirical pattern is therefore better understood as an adaptive interaction over time than as a simple mechanical effect of attack size.

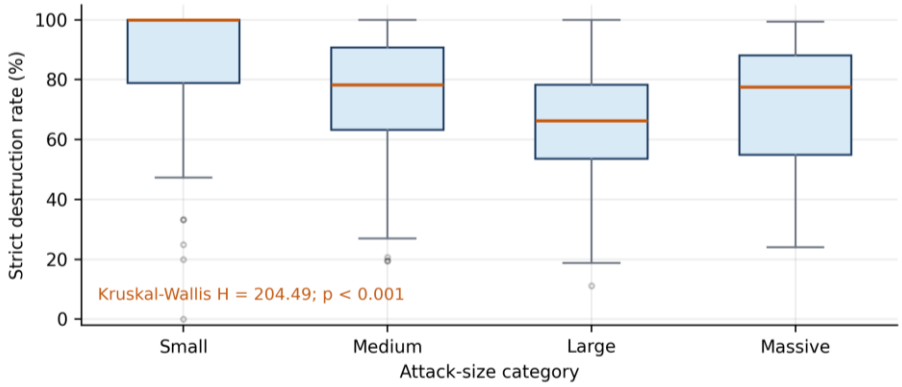

Fig. 4. Strict destruction rates by attack-size category.

Fig. 4 reinforces the group comparison. The Kruskal-Wallis test showed statistically significant differences in strict destruction rates across attack categories ($H = 204.49$; $p < 0.001$) and in capped neutralization rates ($H = 73.27$; $p < 0.001$). These results support the use of attack-size categories as a meaningful analytical variable and confirm that defensive outcomes remain heterogeneous within each group.

Table 5.

Ten largest recorded Shahed-136/131 UAV attack events

Date	Launched	Destroyed	Not reaching the target	Strict rate	Neutral rate
06 Sep 2025	810	747	0	92.22%	92.22%
08 Jul 2025	782	322	423	41.18%	95.27%
24 Mar 2026	703	662	0	94.17%	94.17%
05 Dec 2025	653	585	0	89.59%	89.59%
29 Oct 2025	653	592	0	90.66%	90.66%
22 Dec 2025	635	587	0	92.44%	92.44%
27 Aug 2025	598	563	0	94.15%	94.15%
11 Jul 2025	597	319	258	53.43%	96.65%
28 Nov 2025	596	558	0	93.62%	93.62%
27 Sep 2025	593	566	0	95.45%	95.45%

The largest recorded events demonstrate why the paper avoids a deterministic interpretation of saturation. Some very large attacks had strict destruction rates above 90 percent, while others had lower strict destruction rates but high capped neutralization rates. This pattern suggests that mass attacks can generate pressure, but outcomes depend on mobilization, warning time, route, target distribution, the availability of defensive resources, and non-kinetic effects.

Table 6.

Hypothesis assessment

Hypothesis	Empirical result	Assessment
H1: UAV employment increased over time	Monthly volume increased by +144.71 UAVs/month; $p < 0.001$; $R2 = 0.731$	Strongly supported
H2: Larger attacks reduce destruction rates	Negative bivariate relationship; Spearman rho = -0.406; attack size not significant after controlling for time	Partially supported
H3: Adaptation visible in sustained neutralization	Strict destruction varied, but capped neutralization remained high, and 2026 partial data rebounded.	Mixed but meaningful support

The hypothesis assessment indicates that the article's main empirical contribution is not merely a confirmation of saturation but a more nuanced model. Attack volume clearly escalated. In some tests, larger attacks are associated with lower destruction rates, yet the defense system also shows signs of adaptation through broader neutralization. This combination of escalation, pressure, and adaptation is the study's central empirical pattern.

5. Discussion

5.1 Interpretation of the empirical findings

The results indicate that one-way attack UAV saturation is an operational, economic, and strategic challenge rather than merely a technical air-defense problem. The sharp rise in monthly UAV volume supports the view that Shahed-type UAVs have become a high-volume strike platform. This aligns with external analyses that describe Russia's Shahed campaign as a saturation strategy rather than a sequence of isolated drone attacks [4, 12].

The most important empirical pattern is the coexistence of escalation and adaptation. The number of recorded Shahed-136/131 UAVs increased sharply, yet the broader neutralization rate remained high. This indicates that the defender did not collapse under the increased volume. At the same time, strict destruction rates declined over several years, indicating that both the threat and the defensive response changed. A simple statement that Ukraine either succeeded or failed would therefore be analytically inadequate.

The non-linear pattern across attack categories is significant. If saturation were purely mechanical, the massive category would have the lowest destruction rate. Instead, the large category had the lowest mean strict destruction rate, while massive attacks showed somewhat higher performance. This may indicate surge behavior. When an attack is clearly massive, the defender may mobilize more assets, issue broader alerts, prioritize key areas, and accept higher expenditure.

Large but not extreme attacks may be harder to distinguish from routine patterns and may receive fewer extraordinary defensive resources.

5.2 Implications for small-state air defense

The results suggest that small-state air defense should prioritize endurance and cost-effectiveness. A state with limited inventories cannot assume that high-end interceptors will be available for every incoming UAV. Instead, it needs a tiered system that integrates detection and classification with multiple engagement options: short-range air defense, anti-aircraft guns, electronic warfare, passive protection, rapid repair, and civilian warning systems.

Based on theoretical and empirical analysis, small states should adopt a four-layer counter-UAS planning framework. The first layer is awareness: persistent surveillance, distributed sensors, reporting channels, and public warnings. The second layer is disruption: electronic warfare, navigation interference, deception, and cyber-electromagnetic effects, where legally and technically feasible. The third layer is engagement: mobile fire groups, short-range air defense, guns, interceptor drones, and selective use of missiles. The fourth layer is resilience: hardening, redundancy, repair capacity, and continuity of government and military operations.

This layered logic prevents treating every incoming UAV as a problem for the most expensive air-defense asset. A small state cannot sustain its defense if it defaults to high-end interceptors against low-cost, one-way attack UAVs. The Ukrainian experience suggests that survivability depends on a combination of imperfect measures rather than on a single decisive system.

5.3 NATO interoperability, reporting standards, and military education

In multinational operations or under Article 5, detection data, air-picture management, engagement authority, and resource allocation may involve multiple Allies. NATO IAMD policy emphasizes rapid detection, decision, and engagement across the full threat spectrum, including UAS [7]. To be effective against mass UAV attacks, Allies require common terminology, compatible reporting categories, shared air-picture procedures, and realistic joint training. NATO's counter-drone interoperability exercises underscore that this is already a practical, Alliance-level requirement [31].

Reporting categories matter. If one system records destroyed UAVs, another records neutralized UAVs, and a third does not distinguish decoys from strike UAVs, conducting a multinational assessment becomes difficult. NATO-oriented counter-UAS training should therefore include data literacy and common reporting standards. This is not merely administrative. It affects operational learning, ammunition planning, after-action review, and political communication.

For officer education, the Ukrainian case can be adapted for scenario-based training. Cadets can analyze a month of UAV attacks, calculate destruction and neutralization rates, prioritize the defense of critical nodes, allocate limited assets, and brief commanders on risk. These exercises would link quantitative literacy to operational judgment and prepare future officers for multinational environments where terminology and rules of engagement must be precisely understood.

5.4 Operational indicators for future counter-UAS assessment

The empirical strategy used in this paper can be expanded into a broader operational indicator framework. At a minimum, a mature counter-UAS assessment should distinguish five categories: launch volume, kinetic destruction, non-kinetic neutralization, target effect, and defensive cost. Launch volume captures the scale of pressure. Kinetic destruction captures traditional air-defense performance. Non-kinetic neutralization encompasses outcomes such as electronic warfare, navigation disruption, or failure to reach targets. Target effect captures whether the attack caused military or infrastructure damage. Defensive cost captures the sustainability of the response.

Table 7.

Proposed counter-UAS assessment indicators

Indicator	Operational meaning	Planning relevance
Launch volume	Number and frequency of incoming UAVs	Pressure on sensors, personnel, and command systems
Strict destruction	UAVs kinetically destroyed	Traditional air-defense performance
Neutralization	UAVs destroyed or failed to reach the target	Broader defensive effect, including non-kinetic outcomes
Target effect	Damage or disruption caused by successful UAVs	Infrastructure and operational resilience
Defensive cost	Resources expended to defeat or neutralize UAVs	Sustainability and cost-exchange ratio

Such a framework would move analysis beyond the binary question of whether a drone was shot down. A month with a lower destruction rate, a high neutralization rate, and limited target damage may indicate an effective layered defense. Conversely, a month with a high destruction rate but excessive use of high-end interceptors may indicate a tactically successful but strategically costly response. This distinction is particularly important for small states, where sustainability often matters more than single-event performance.

5.5 Military education and officer training

The findings have direct implications for military education. Future officers should be trained to interpret UAV attacks as combined operational events rather than isolated technical incidents. This includes understanding how UAS interact with intelligence, surveillance, and reconnaissance, electronic warfare, cyber effects, civil infrastructure, logistics, and public communication. The ability to interpret data, assess trends, and understand saturation logic is therefore a professional competence, not merely a specialist air-defense skill.

Scenario-based training can translate these findings into officer education. Cadets can receive monthly attack data, calculate destruction and neutralization rates, identify changes in attack volume, prioritize critical infrastructure, and recommend counter-UAS resource allocation. Such exercises would integrate quantitative literacy, operational judgment, and NATO-style briefing skills. They would also strengthen interoperability by familiarizing officers with common reporting categories and evidence-based decision-making.

5.6 Strategic communication and deterrence

Drone saturation also has a diplomatic and strategic-communication dimension. Public reporting on destruction and neutralization rates affects public confidence, allied support, and adversary perceptions. If a state reports only the number of drones destroyed, it may understate the effectiveness of electronic warfare and other defensive measures. If it reports broad neutralization figures without methodological clarity, it may undermine credibility. Transparent terminology is therefore part of deterrence and public resilience.

A final strategic point concerns adversary incentives. If an attacker believes that mass UAV attacks can exhaust defenses at an acceptable cost, it may invest in large-scale production and sustain repeated pressure. If small states demonstrate layered, resilient, and cost-effective counter-UAS systems, the expected utility of such attacks may decline. Resilience is therefore not only defensive but also deterrent. It signals that low-cost saturation will not easily lead to strategic paralysis.

5.7 Limitations

Several limitations must be acknowledged. First, the dataset is based on public reporting and official Ukrainian Air Force figures compiled in an open dataset. It is suitable for identifying macro-level trends but cannot independently verify every engagement. Second, the Shahed-136/131 category may include strike UAVs, decoys, or related systems, depending on reporting practices. Third, the 'not reaching the target' category does not specify the causal mechanism and should not be automatically attributed to electronic warfare.

Fourth, the 2026 data are partial and end on 4 April 2026 in the analyzed file. Annual comparisons involving 2026 must therefore be treated cautiously. Fifth, the analysis does not include direct financial cost data, target categories, or geographic distribution. These variables would enable a more robust assessment of cost-exchange ratios and effects on critical infrastructure. Despite these limitations, the study provides a transparent, reproducible empirical basis for examining UAV saturation and air defense adaptation in a major contemporary conflict.

5.8 Practical recommendations for small-state defense planning

The analysis supports five practical recommendations. First, small states should establish a national counter-UAS reporting standard before a crisis. Categories such as launched, destroyed, neutralized, decoy, failed, and target effect should be consistently defined. Second, national exercises should include repeated-night UAV saturation scenarios rather than isolated drone incidents. Third, air-defense planning should include critical infrastructure network analysis, because dispersed substations, depots, bridges, and communication nodes may be strategically important even if individually small.

Fourth, procurement should prioritize layered, cost-effective effects. High-end interceptors must remain available for high-end threats. At the same time, low-cost drones should be countered through scalable combinations of sensors, electronic warfare, guns, mobile teams, interceptor drones, and passive protection. Fifth, small states should integrate counter-UAS lessons into officer education, staff training, and civil-military crisis planning. Recent European anti-drone and 'drone wall' initiatives show that this is becoming a regional defense priority, not merely a national procurement issue [33, 34]. The decisive question is not only whether a state can destroy drones but also whether it can maintain defense, public confidence, and alliance interoperability under repeated pressure.

6.Conclusions

This paper examined the relationship between one-way attack UAV saturation and air defense adaptation through a quantitative analysis of UAV attacks involving Shahed-136/131 UAVs against Ukraine. The empirical evidence strongly supports H1. The scale of recorded UAV employment increased substantially, with the monthly volume rising by approximately 144.71 UAVs. The annual data show the sharpest escalation in 2025, with 54,796 UAVs launched.

H2 is partially supported. Larger attacks were associated with lower strict destruction rates in bivariate and rank-order analyses, but the effect of attack size was not significant after controlling for time. H3 receives mixed but meaningful support. Strict destruction rates declined at times during the campaign, while broader neutralization remained high. Partial 2026 data indicate a rebound in strict destruction performance.

The paper's main contribution is threefold. First, it operationalizes UAV saturation through attack volume and defensive performance indicators. Second, it distinguishes kinetic destruction from broader neutralization. Third, it links the Ukrainian empirical case to small-state air defense planning within NATO. The central lesson is that countering one-way attack UAVs requires not only shooting down drones but also maintaining a layered, cost-effective, and interoperable defense over time.

Future research should integrate attack-volume data with target categories, cost estimates, geographic distribution, and a clearer distinction among strike UAVs, decoys, and other aerial systems. This approach would enable a more precise assessment of the cost-exchange relationship between low-cost one-way attack UAVs and the systems used to defeat them. For defense planners, the practical implication is immediate. Counter-UAS preparedness should be evaluated not by a single success rate but by a balanced set of indicators measuring pressure, effect, cost, and adaptability.

Acknowledgements. The author declares that no external funding was received for this research. The empirical analysis uses publicly available open-source data. All interpretations, conclusions, and possible errors remain the sole responsibility of the author.

References

1. **Ivaniuk P**. Massive Missile Attacks on Ukraine. Kaggle Dataset. Available online: https://www.kaggle.com/datasets/piterfm/massive-missile-attacks-on-ukraine/data.
2. **Center for Strategic and International Studies**. Russian Firepower Strike Tracker: Analyzing Missile Attacks in Ukraine. Available online: https://www.csis.org/programs/futures-lab/projects/russian-firepower-strike-tracker-analyzing-missile-attacks-ukraine.
3. **Center for Strategic and International Studies**. Assessing Russian Firepower Strikes in Ukraine. Available online: https://www.csis.org/analysis/assessing-russian-firepower-strikes-ukraine.
4. **Center for Strategic and International Studies**. Drone Saturation: Russia's Shahed Campaign. Available online: https://www.csis.org/analysis/drone-saturation-russias-shahed-campaign.
5. **Center for Strategic and International Studies**. Calculating the Cost-Effectiveness of Russia's Drone Strikes. Available online: https://www.csis.org/analysis/calculating-cost-effectiveness-russias-drone-strikes.
6. **NATO Integrated Air and Missile Defence Centre of Excellence**. NATO IAMD COE. Available online: https://iamd-coe.org/.
7. **NATO**. NATO Integrated Air and Missile Defence Policy. Available online: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy.
8. **NATO**. Integrated Air and Missile Defence. Available online: https://www.nato.int/en/what-we-do/deterrence-and-defence/nato-integrated-air-and-missile-defence.
9. **Joint Air Power Competence Centre**. A Comprehensive Approach to Countering Unmanned Aircraft Systems. Kalkar: JAPCC. Available online: https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/.
10. **U.S. Department of Defense**. Counter-Small Unmanned Aircraft Systems Strategy. Washington, D.C.: Department of Defense, 2021. Available online: https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf.
11. **International Institute for Strategic Studies**. The Uninhabited War in Ukraine. Available online: https://www.iiss.org/globalassets/media-library---content--migration/files/publications---free-files/strategic-dossier/uavs-2026/iiss_ch-3-uavs-isr-deterrence-and-war_032026.pdf.
12. **Institute for Science and International Security**. Monthly Analysis of Russian Shahed-136 Deployment Against Ukraine. Available online: https://isis-online.org/isis-reports/monthly-analysis-of-russian-shahed-136-deployment-against-ukraine.
13. **Reuters**. Russian Drones Swarm Smaller Ukrainian Power Stations, Data Shows. Available online: https://www.reuters.com/business/aerospace-defense/russian-drones-swarm-smaller-ukrainian-power-stations-data-shows-2026-05-08/.

14. **Reuters**. Ukraine Says It Is Running Short of Air Defence Missiles. Available online: https://www.reuters.com/business/aerospace-defense/ukraine-says-it-is-running-short-air-defence-missiles-2026-05-08/.
15. **Council on Foreign Relations**. Can Iranian Drones Turn Russia's Fortunes in the Ukraine War? Available online: https://www.cfr.org/articles/can-iranian-drones-turn-russias-fortunes-ukraine-war.
16. **European Defence Agency**. UAS Integration. Available online: https://eda.europa.eu/what-we-do/all-activities/activities-search/uas-integration.
17. **EUROCONTROL**. Unmanned Aircraft Systems. Available online: https://www.eurocontrol.int/unmanned-aircraft-systems.
18. **RAND Corporation**. The Implications of the Fighting in Ukraine for Future U.S. Defense Planning. Santa Monica: RAND Corporation. Available online: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3100/RRA3141-2/RAND_RRA3141-2.pdf.
19. **Field A. Discovering Statistics Using IBM SPSS Statistics**. 5th ed. London: SAGE Publications, 2018.
20. **Wooldridge J.M**. Introductory Econometrics: A Modern Approach. 7th ed. Boston: Cengage Learning, 2019.
21. **Hyndman R.J**., Athanasopoulos G. Forecasting: Principles and Practice. 3rd ed. Melbourne: OTexts, 2021.
22. **McKinney W**. Python for Data Analysis: Data Wrangling with pandas, NumPy, and Jupyter. 3rd ed. Sebastopol: O'Reilly Media, 2022.
23. **Chaari M.Z**. Analysis of the Power of Drones and Limitations of the Anti-Drone Solutions. Security and Defence Quarterly. Available online: https://securityanddefence.pl/Analysis-of-the-power-of-drones-and-limitations-of-the-anti-drone-solutions-on-the%2C208347%2C0%2C2.html.
24. **Dobija K**. Countering Unmanned Aerial Systems in Military Operations. Security and Defence Magazine. Available online: https://sd-magazine.eu/index.php/sd/article/view/195.
25. **Grigoraș C**., Musat O. Countering Unmanned Aircraft Systems - A Multi-Domain Effort. Available online: https://www.researchgate.net/publication/382008757_Countering_Unmanned_Aircraft_Systems_-_A_Multi-Domain_Effort.
26. **Ciolponea C.A**. The Integration of Unmanned Aircraft System in Current Combat Operations. Available online: https://www.armyacademy.ro/reviste/rev4_2022/Art_Ciolponea.pdf.
27. **Object Detection Models in Counter-Unmanned Aircraft Systems**. Available online: https://ceur-ws.org/Vol-4048/paper25.pdf.
28. **NATO Science and Technology Organization**. Countering Autonomous Threats / Counter-Unmanned Aircraft Systems. Available online: https://www.sto.nato.int/document/countering-autonomous-threatscounter-unmanned-aircraft-systems-c-uas-presentation/.
29. **U.S. Army**. ATP 3-01.81 Counter-Unmanned Aircraft System Techniques. Washington, D.C.: Headquarters, Department of the Army. Available online: https://aviation-assets.info/wp-content/uploads/ARN3099_ATP-3-01x81-FINAL-WEB.pdf.
30. **Congressional Research Service**. Department of Defense Counter Unmanned Aircraft Systems. Available online: https://www.everycrsreport.com/reports/R48477.html.
31. **NATO**. Ukraine Joins NATO Counter-Drone Exercise for First Time. Available online: https://www.nato.int/en/news-and-events/articles/news/2024/09/19/ukraine-joins-nato-counter-drone-exercise-for-first-time.
32. **International Partnership for Human Rights**. Terror in the Details: Western-Made Components in Russia's Shahed-136 Attacks. Available online: https://stories.iphronline.org/terror-in-the-details/index.html.
33. **Reuters**. PGZ, Estonia's Frankenburg to Build Anti-Drone Defence Plant in Poland. Available online: https://www.reuters.com/business/aerospace-defense/pgz-estonias-frankenburg-build-anti-drone-defence-plant-poland-2026-03-27/.
34. **Associated Press**. European Ministers Move Ahead with Drone Wall Project. Available online: https://apnews.com/article/0330c4d8ca34659626d85a39ff03828f.