ADG CONSULT NZ

DEFENCE CAPABILITY | DOCTRINE DEVELOPMENT | REGIONAL SECURITY

UNCREWED AERIAL SYSTEMS IN SOUTHEAST ASIAN DEFENSIVE OPERATIONS

Tactical realities, contested communications and the transfer of Ukrainian operational lessons to national doctrine



PROFESSIONAL DISCUSSION PAPER

01 NOVEMBER 2026 | VERSION 2.0

Prepared as an ADG Consult NZ analysis for consideration by Southeast Asian defence institutions and Ukrainian subject-matter partners.

Document control and use

Document	Description
Publication	ADG Consult NZ — Defence Doctrine & Capability Insight
Title	Uncrewed Aerial Systems in Southeast Asian Defensive Operations
Edition	Version 2.0 | 1 November 2026
Classification	Unclassified. Based on publicly available information and explicit analytical inference.
Purpose	Support senior defence discussion, nationally owned capability development, lessons analysis, training design and validation.
Status	Independent discussion paper; not an official military doctrine, country policy, authorised SOP or training agreement.
Image policy	Cover and conceptual diagrams are original illustrations. They are not presented as photographic or cartographic evidence of events.

The paper assesses the strategic and tactical implications of surveillance, information exploitation, identification and armed UAS in Southeast Asian defence. Its practical recommendations concern governance, system assurance, training design, evidence quality and institutional adaptation. It deliberately does not prescribe detailed attack procedures, target selection sequences, electronic-warfare countermeasures or unit dispositions. These require duly authorised national processes and, where applicable, classified doctrine.

Terminology: the war between Russia and Ukraine began in 2014, and the full-scale invasion began on 24 February 2022. On the publication date the full-scale conflict has continued for approximately four years and eight months.

Contents

PART I THE DEFENCE PROBLEM

Executive assessment

1–4 Scope, evidence, regional terrain and the UAS enterprise

PART II INFORMATION UNDER PRESSURE

5–9 Communications, EW, weather, surveillance and identification

PART III TERRAIN & MISSION APPLICATION

10–14 Constrained corridors, rivers, islands, armed UAS and counter-UAS

PART IV BUILDING A RESILIENT FORCE

15–21 Sustainment, command integration, training, tests, procurement and principles

PART V UKRAINE–SOUTHEAST ASIA KNOWLEDGE TRANSFER

22–27 Advisory partnership, national doctrine, SOP architecture and roadmap

28 Conclusions and recommended direction

ANNEXES

A Documented Ukraine operational vignettes and lessons learnt

B Fictional Southeast Asian field exercises for validation

C Evidence and uncertainty matrix

D Proposed national SOP portfolio and assurance checklist

E Ukrainian practitioner interview and lessons-capture protocol

F References and reading list

Executive assessment

Modern uncrewed aerial systems (UAS) can materially improve military awareness, shorten the time needed to recognise changing conditions and reduce the requirement to expose personnel to some reconnaissance tasks. Their tactical value is real. Equally real is the possibility that the entire system will perform poorly once enemy action, tropical weather, complex terrain, disrupted satellite navigation, congested radio spectrum and sustained operational demand are introduced. The decisive distinction is not between possessing drones and lacking drones; it is between fielding an aircraft fleet and fielding a dependable reconnaissance, command and support capability.

The Russia–Ukraine War has supplied a powerful body of operational evidence. Uncrewed systems have become central to reconnaissance, monitoring of movement, assessment of battlefield changes and armed effects. They have also driven a continuous contest of adaptation and counter-adaptation in radio communications, electronic warfare (EW), protection and sustainment. The Australian Army Research Centre's 2026 study makes the important methodological point that Ukrainian lessons must be interpreted in context rather than transplanted unchanged to other theatres. That proposition is particularly important in Southeast Asia, where forest canopy, monsoon rainfall, tidal rivers, marshland, mountain barriers, island separation and civilian river traffic differ sharply from the frequently open agricultural and urban terrain of eastern and southern Ukraine. [1][2][3]

The most consequential weakness in many peacetime UAS programmes is an assumption of continuous connectivity. Three distinct pathways must succeed: the aircraft must remain safely controllable; useful sensor information must be received and understood; and the information must then reach an authorised decision-maker in time to influence events. These pathways may fail independently. A flight may be completed while its sensor product is unusable. A clear video feed may not establish where an object is located. A well-observed event may never reach the commander. Conversely, some tasks may be completed safely and usefully without continuous high-bandwidth imagery. Doctrinal design must distinguish these outcomes.

The narrow corridors created by mountain roads, jungle tracks, bridges, causeways and settlement belts increase the significance of observation and infrastructure status. They also produce unusually difficult identification problems: civilian vehicles use the same routes, foliage and relief interrupt lines of sight, and observation from a single angle rarely reveals the whole environment. River defence introduces additional challenges because channels, sandbars, riverbanks, currents, flooding, ferries and civilian livelihoods change across hours and seasons. UAS may provide useful warning and situational assessment in both settings, but imagery alone cannot establish control of a corridor or water barrier.

This paper proposes a doctrine based on eight principles: mission before platform; information quality before image volume; explicit link-degradation assumptions; weather and terrain realism; human command accountability; combined-arms and inter-service integration; measured sustainment; and continuous contested-environment testing. It considers surveillance, target identification and direct-attack UAS as distinct capability categories. The armed category is assessed in terms of military role, governance, reliability and humanitarian constraints rather than detailed attack techniques. None of these principles is technologically fashionable; each is necessary to prevent a peacetime success story becoming a wartime failure.

1. Purpose, operational frame and method

The purpose of this paper is to establish a defensible foundation for evaluating and developing the tactical employment of UAS in Southeast Asian land defence. The focus is not on whether a particular drone is commercially attractive, inexpensive or sophisticated. It is whether UAS can remain useful in the operational environment for which forces intend to rely upon them. The framework applies to land formations, territorial defence forces and relevant supporting maritime and air components. It also addresses the civil–military interface because roads, waterways, airspace and communications infrastructure in the region are extensively shared with civilian users.

The term unmanned aerial vehicle (UAV) denotes the aircraft. Uncrewed aerial system (UAS) denotes the aircraft together with its control equipment, datalinks, sensors, software, power, operators, analysts, maintainers and operating procedures. This distinction is essential. Aircraft performance on a test range is not evidence of end-to-end tactical performance. A camera's theoretical recognition range is not evidence that the image will support accurate identification in rain or haze. A manufacturer's nominal endurance is not proof of useful sortie duration under tropical heat and adverse winds.

The evidence base combines publicly available analyses of the Ukraine war from the Royal United Services Institute (RUSI), Australian Army Research Centre, International Institute for Strategic Studies (IISS) and Center for Strategic and International Studies (CSIS), with environmental and safety references from the World Meteorological Organization (WMO), International Telecommunication Union (ITU), Mekong River Commission, International Civil Aviation Organization (ICAO) and International Committee of the Red Cross (ICRC). Sources vary in method and confidence. Research based on practitioner interviews is invaluable but does not automatically yield universal statistics. Public descriptions of exceptional successful drone strikes are affected by selection and publicity bias; destroyed or failed drones rarely generate equivalent attention. [1][2][3][4]

The analysis therefore separates three categories of proposition. Observed lessons are findings consistently supported by reputable conflict reporting. Regional deductions are reasoned inferences about Southeast Asian geography, climate and infrastructure that require national validation. Unverified assumptions are matters that cannot be responsibly certified without realistic field trials, military-grade data, or operational experience under an opposing force. The proposed framework is intended to turn the third category into testable evidence rather than unexamined doctrine.

2. What Ukraine has actually taught

The war in Ukraine did not reveal a static 'drone revolution' in which a single technical solution transformed all ground combat. Instead it revealed a continuing military competition. In the opening years, commercially adapted small aircraft demonstrated that relatively inexpensive sensors could provide local observation and support rapid adaptation. By 2024, both sides were increasingly incorporating reconnaissance and strike UAS into combined-arms processes while simultaneously contesting access to the electromagnetic spectrum. RUSI's February 2025 fieldwork emphasised adaptation across reconnaissance, close combat, logistics, engineering and air defence rather than presenting drones as an independent arm capable of replacing those functions. [2]

By 2025 and 2026, the evidence was more demanding still. The IISS identified the susceptibility of off-board radio links to disruption, while the Australian Army Research Centre described the growing requirement for specific aircraft types, workforce specialisations, sustainment systems and rapid technical learning. The threat to UAS was no longer primarily technical malfunction. It included opponents deliberately seeking to interfere with communications, navigation and the functioning of the broader UAS enterprise. These developments mean a nation beginning its capability development in 2026 should not imitate the most visible equipment of 2022 as though the contest had stood still. [1][3]

Several lessons are transferable across theatres. Firstly, repeated observation changes decision-making only when it is integrated with the command system and when its limitations are understood. Secondly, the electromagnetic environment must be treated as contested from the outset, not as a later technical complication. Thirdly, trained teams, maintainers, analysts and spare parts determine operational endurance just as much as available airframes. Fourthly, UAS are exposed to a cycle in which an advantage invites an opposing response. Fifthly, the psychological effect of persistent aerial observation is substantial but must not be confused with control of territory or proof of enemy intentions. [1][5]

Other conclusions are much less portable. The scale of publicly reported drone use and associated losses is shaped by the Ukrainian front's particular geography, equipment availability, industrial adaptation, air-defence environment and the duration of a large conventional war. Claims that one platform class has made other arms obsolete are not borne out by the breadth of the reported fighting. An archipelagic state's problem may include

isolated island garrisons, heavy coastal cloud, limited engineering access and weak electrical infrastructure. A mainland Southeast Asian force may contend with mountainous forest, irrigation networks, settlements and highly seasonal rivers. Neither problem can be solved merely by reproducing Ukrainian equipment inventories or tactical vocabulary.

The appropriate lesson is organisational rather than ideological: form hypotheses from Ukrainian experience, expose them to rigorous field testing in local conditions and update procedures at a rate that reflects the threat. The enemy adapts; therefore a doctrine that can be changed and tested quickly is more valuable than one that claims a permanently superior method.

3. The Southeast Asian operating environment is not one environment



Figure 1 | Southeast Asian geography creates dissimilar operating conditions and distinct assurance cases for UAS operations.

Southeast Asia contains at least five operationally distinct terrain families relevant to UAS: highland forests and steep valleys; tropical lowland jungle and plantations; river plains and delta complexes; dense metropolitan and peri-urban corridors; and littoral or island environments. Each creates a different relationship between visibility, communications, mobility and support. A standard procurement requirement that assumes a single nominal range, endurance and sensor performance would mask these differences and lead to inaccurate force-planning conclusions.

In upland forest, relief can obscure movement and interrupt terrestrial radio paths even when an aircraft is geographically close to its ground element. Dense canopy prevents confident assessment of activity beneath trees and can confuse thermal interpretation, particularly when humidity, ground temperatures and vegetation reduce contrast. A sensor may identify a disturbed clearing while being unable to determine its origin or present use. Monsoon rainfall can rapidly close airfield approaches, prevent safe recovery and change the risk of access roads used by crews. Limited roads compound the difficulty of maintenance and battery replenishment.

Lowland jungle, plantations and mixed settlements differ from highland forest. Canals and levees may make ground routes appear continuous on a map while being discontinuous for military vehicles. Commercial agriculture creates regular geometric shapes that can be mistaken for evidence of human engineering activity unrelated to its ordinary use. Houses, religious institutions, schools, agricultural sites and commercial river traffic are intermingled with the areas in which military observation may be required. This increases the likelihood of false interpretation and raises the need to preserve legal distinctions between civilian activity and military objectives.

Urban corridors offer infrastructure and multiple visual landmarks but create dense radio congestion, screening from buildings, hazardous flight obstacles and extensive civilian movement. Coastal and

archipelagic settings offer wide horizontal visibility in some conditions, but over-water weather, saline corrosion, sea spray, separated maintenance bases and the security of communications infrastructure can dominate system availability. It is therefore inaccurate to discuss a single 'tropical drone doctrine'. The appropriate national doctrine must define common fundamentals while requiring theatre-specific qualification.

Seasonality is not a footnote. The Mekong River Commission identifies monsoon-driven flood pulses and individual storm events as central features of the region's hydrology. The WMO's 2026 report on Asia's 2025 climate documents severe tropical rainfall and flooding affecting Southeast Asian countries. A capability rated only in fair-weather trials has not yet established its fitness for a region in which the weather may alter both air operations and the ground situation being observed. [6][7]

4. Understanding the UAS enterprise rather than the aircraft

A deployable UAS capability comprises several interacting elements: airframes; sensors; command and control; control and payload communications; geospatial and time references; trained personnel; intelligence analysis; maintenance; power; airspace management; security; logistics; and a mechanism for learning from failures. A fleet can achieve a high technical serviceability rate while delivering little decision advantage because one or more of the other elements is weak. This is a central force-development risk for organisations that measure progress primarily by purchased aircraft numbers or pilot qualifications.

At tactical level, the useful unit of measurement should be the *validated mission outcome*. For surveillance, that may mean a timely, correctly qualified observation that is received by its intended user. For infrastructure assessment, it may mean a documented determination that a bridge, crossing, route or landing area remains usable within stated limits. For communications support, it may mean verified exchange of relevant information between authorised users despite partial disruption. Armed systems require additional evidence concerning command authority, identification, legality, safety, positive control and abort or fail-safe behaviour. Merely launching or landing a system does not establish any of these outcomes.

People constitute the most difficult element to surge quickly. A competent remote pilot is not necessarily a competent imagery analyst, network maintainer, geospatial specialist, meteorological assessor or commander. Training a large number of operators without establishing these supporting functions creates a narrow and fragile capability. The Ukrainian experience demonstrates the need for formal specialisations and practical adaptation processes, but national force design should avoid copying a foreign organisational chart before defining the missions, personnel pipeline and support capacity of the local force. [1]

The principle of mission primacy should be applied in every acquisition and training decision. A requirement for routine route-condition assessment might need high reliability and rapid reporting more than maximum sensor resolution. Assessment of flooding may favour consistency and accurate georeferencing over continuous video. Observation along a built-up riverbank may demand better contextual identification rather than longer aircraft range. Capabilities should be judged by the quality and safety of the task accomplished, not by the number of specifications that a vendor can display.

5. Communications: the central tactical weakness



Figure 2 | Three distinct reliability problems in one UAS mission — control, sensor data and command reporting.

Communications are not merely an accessory to a UAS; they are part of the military effect. Three communication functions should be defined separately. Aircraft command and control allows authorised operators and supporting software to maintain the safe control of the vehicle. Payload information transfer carries still imagery, video, sensor records and associated metadata. Operational information distribution carries interpreted products, task status and reports to the soldiers, headquarters or other agencies that need them. Each function has a different bandwidth requirement, timeliness requirement and failure consequence. Treating them as a single 'link' obscures operational risk.

In a tropical valley, an aircraft may have intermittent or obstructed connectivity even in the absence of hostile electronic warfare. Hillsides, vegetation, infrastructure and weather affect terrestrial propagation in frequency-dependent ways. ITU Recommendations P.530 and P.837 provide technical foundations for evaluating line-of-sight systems and rainfall characteristics, but they do not substitute for measurement at the intended operating location. They also should not be misused as a claim that all rain affects all drone links equally. Carrier frequency, path geometry, antenna installation, equipment design and the wider physical environment matter. [8][9]

In the presence of an enemy, normal physical constraints are compounded by deliberate interference and deception. Interference may affect control, imagery, position information, time synchronisation or the means by which reports are redistributed. Navigation can appear plausible while being wrong. The more dangerous failure is often not an obvious blackout, but a system that displays stale, displaced or apparently precise information without adequately identifying its uncertainty. The European Union Aviation Safety Agency's July 2026 GNSS safety bulletin underscores the continuing importance of recognising and training for navigation-system degradation. [10]

Communications doctrine should be written around degraded modes, with explicit descriptions of which tasks remain authorised and meaningful when control, payload or distribution services are lost. The organisation should know how to distinguish current information from delayed information, known positions from uncertain positions, observations from inferences, and confirmed reports from uncorroborated reports. Systems should preserve timestamps, source provenance and operator annotations. Commanders must not interpret a coloured icon on a display as proof that the underlying observation is current, correctly positioned or independently verified.

Communications architecture is also an organisational issue. A ground observer may see an important change but have no functioning pathway to an engineer or route authority. An aircraft may return with useful imagery that is processed too late to influence a decision. Two adjacent formations may employ incompatible map

references, software or classification rules. All such failures should be counted as failures of tactical information delivery even if the aircraft itself completes its mission. A mature doctrine includes minimum reporting formats and explicit ownership of data quality, as well as approved routes for sharing material across military services and civilian authorities when relevant.

The practical emphasis should be on tested resilience rather than a promise of uninterrupted video. High-resolution live imagery is attractive but can impose substantial dependency on bandwidth and continuous connectivity. Some decisions can be supported by smaller, well-qualified reports; others genuinely require moving imagery or different sensors. The commander needs to understand what information has been lost when the network degrades and what conclusions can no longer safely be drawn. This paper deliberately does not prescribe methods for defeating opposing EW systems or sustaining weapon-control links through specific hostile interference patterns; such activities require authorised, controlled development and testing.

ADG analysis | Operational implications and required proof

A headquarters that receives UAV video in a command post but cannot distribute a reliable intelligence report to a subordinate formation has not solved the communications problem. End-to-end assessment must trace the information from tasking, through the airborne platform and operator, to interpretation, dissemination, acknowledgement and subsequent correction. These stages should have distinct owners and records. A control link, a payload link and a headquarters communication service may depend upon different infrastructure and can fail at different times. No single display provides adequate proof of their combined availability.

The most dangerous failure is often graceful degradation that goes unnoticed. An aircraft may continue a pre-set activity, a screen may freeze on the last received frame, or an analyst may continue viewing a delayed recording while the command system assumes that the picture is live. National reporting formats should require observation time, time of receipt, source, estimated position quality, confidence, missing sectors and the age at which information ceases to support the decision. The doctrine must require an explicit distinction between “not observed”, “observed absent” and “unable to observe”.

In restricted valleys or built-up corridors, the link problem is geographical as well as electromagnetic. Terrain relief and surrounding structures may obstruct a communication path while navigation and camera electronics continue to operate. A peacetime success report based on good-weather line-of-sight flying therefore provides little assurance of wartime performance. Evaluations should record coverage, interruptions, restart behaviour, logging completeness and the ability to deliver the final report to the intended headquarters. For defensive forces this is a command-reliability issue before it is a procurement specification. [1][2][8]

6. The electromagnetic battlespace: own-force effects and enemy action

Electronic warfare is often discussed as though an adversary operates a device that either disables a drone or fails to do so. The actual interaction is more complex. The relevant environment includes civilian emitters, friendly radios, aviation services, satellite-navigation dependence, commercial infrastructure, opposing electronic activity and UAS of different technical designs. The same spectrum use that enables military coordination can interfere with another friendly activity. The Australian Army Research Centre's 2026 study and UNIDIR's October 2026 publication both describe EW as a persistent adaptive contest that affects technological choices and institutional preparedness. [1][11]

For Southeast Asian forces, the first planning obligation is therefore to establish a realistic electromagnetic baseline. This is not a single map of 'good' and 'bad' coverage. Conditions differ across terrain, weather, nearby equipment, time and operational activity. A system that works during a clean test may experience poor performance once military radios, vehicles, maritime users and other UAS are active in the same area. Exercises should assess the consequences of friendly interference and equipment interoperability before

adding an opposing force. Otherwise a unit may attribute routine configuration or deconfliction problems to enemy sophistication while failing to correct them.

An untested EW environment should be declared as an uncertainty rather than silently assumed away. A training report that states 'UAS mission successful' without recording the level of radio congestion, GNSS availability, relevant friendly emitters and opposing interference has limited operational value. Conversely, a trial that records loss of performance under disruption can be highly successful as a learning activity. Its output is evidence for changed requirements, doctrine and training. There is little institutional value in protecting a system's reputation by avoiding realistic conditions.

Electronic and navigation failures demand incident discipline. Operators and analysts must be able to report anomalies without speculation; maintainers need access to fault records; and headquarters need a method for determining whether failures indicate equipment limitations, configuration problems, weather, interference or adversary activity. It is not always possible to identify the cause promptly. Doctrine should make that uncertainty visible. False certainty encourages both technical misdiagnosis and operationally unsafe decisions.

The larger lesson is that military confidence must be conditional. A UAS-qualified formation may perform well in clear conditions with cooperative communications, moderately under congestion and badly when several stressors coincide. All three results can be valid. Realistic readiness reporting should disclose the conditions under which an assessed level of capability has been demonstrated. A standard that rewards only successful sorties incentivises unrealistic exercises; a standard that rewards honest understanding of failure modes produces better force development.

ADG analysis | Operational implications and required proof

Electronic warfare should be treated as a mission environment rather than an exotic enemy capability that appears only in advanced exercises. The competing forces in Ukraine have used the electromagnetic spectrum for communications, sensing, navigation, interference and protection. RUSI's study of Ukraine's 2023 offensive identifies friendly-spectrum interference as a serious combined-arms problem: expanding the number of electronic systems without a coordinated management framework can degrade a force's own capability. The distinct lesson is not to prescribe a universal countermeasure, but to establish spectrum responsibilities, safe test conditions, logged outcomes and joint review. [18][19]

There is no defensible public basis for asserting that a specific Southeast Asian force will experience the same jamming patterns or that a commercial link shown to function in Europe will remain serviceable under a different opponent and terrain. Many militaries in the region have no combat-validated baseline against a technologically capable adversary. Such uncertainty must be represented in readiness statements. National trials should expose flight crews, communications staff, intelligence cells and commanders to approved simulations of degraded connectivity and conflicting information, without making dangerous interference experiments on public networks.

EW resilience includes institutional discipline: knowing what failed, knowing whether it was accidental interference, environmental attenuation or hostile action, and ensuring the assessment is not altered to fit an expected successful result. A credible exercise evaluation should use independent observers, a declared safety envelope, qualified spectrum professionals and a formal procedure for stopping tests. Electronic-protection claims should remain limited to the conditions actually demonstrated. [11]

7. Weather, terrain and sensor limitations

Aerial visibility is not equivalent to observation beneath canopy, nor is a clear-looking image equivalent to accurate recognition. Tropical vegetation, shadow, cloud base, rain, haze, steam, water reflection and urban screening affect the information delivered by electro-optical and thermal sensors. The practical consequence is a need to qualify not only the aircraft but also the *claim being made about the scene*. Detecting activity,

classifying a broad object category, identifying a particular object and understanding its intention are four different analytical achievements. They should not be merged into one label such as 'target acquired'.

Thermal imagery can assist in some low-light tasks but should not be treated as a universal solution to jungle observation. Vegetation conceals and mixes heat signatures; daily heating alters contrasts; and warm, humid conditions can reduce interpretive clarity. A bright point or moving shape does not independently identify a person as a combatant or an object as military. Multi-sensor or repeat observation may improve confidence, but the extent of improvement depends on conditions and must be measured rather than assumed.

Wind and rainfall present both aviation and information risks. A platform may remain technically flyable while sensor motion, moisture, reduced visibility or the need to terminate early makes the product unusable. Ground access to launch and recovery areas may fail before the aircraft's endurance limit is reached. A riverine mission conducted during dry-season low water may have little predictive value for high-water conditions when currents, floating debris and available riverbank sites are different. For archipelagic forces, salt exposure, storage conditions and transport damage can degrade availability even before a sortie begins.

The appropriate performance statement is a conditional one: under a clearly defined terrain, weather and communications envelope, a trained team demonstrated a stated quality of information at a stated reliability. Anything stronger should require stronger evidence. National test establishments should maintain representative local datasets rather than accepting a manufacturer's marketing imagery or a foreign trial as sufficient proof of field performance.

ADG analysis | Operational implications and required proof

Tropical rain is not merely an obstacle to flight. It changes the information task. In a river valley, rainfall alters water levels, sediment movement, channel visibility and civilian activity. Over a plantation it changes surface reflectivity; in upland forest it can produce rapid fog, low cloud and mud damage to access roads. Heat, moisture and marine salt also affect equipment storage, electrical connectors, batteries and repair practice. These phenomena interact: a delayed flight may mean that the bridge, ferry landing or road cut has changed by the time a report reaches the commander.

Sensor confidence should be evaluated empirically, using known ground truth and blinded review rather than assumptions based on nominal resolution. A usable test set would include visually similar military and civilian vehicles where legally and safely simulated, partial canopy obstruction, reflective water, rain-streaked imagery, low contrast, changing light and imperfect time/position metadata. The primary question is whether an assessor knows what cannot be concluded. A system that produces excellent video but repeatedly encourages false identification has failed the national intelligence requirement. [6][7][9]

8. Surveillance and reconnaissance: what a commander should expect

Surveillance is a process of sustained observation for a defined information purpose; reconnaissance is the directed acquisition of information about a particular question or area. Both may be supported by UAS, but neither is synonymous with flying over the scene. The requirement must identify what decision needs support, what would count as a useful observation, when it is needed and how uncertainty will be communicated. Without those elements an aircraft may generate impressive footage without improving tactical understanding.

In Southeast Asian defensive operations, particularly valuable non-kinetic outputs may include changing road and bridge conditions, the movement of floodwater, the use of public roads by civilians, visibility of ferry approaches, disruption of communications infrastructure, natural obstacles, wildfire or smoke, and signs of damage to key facilities. A UAS may also contribute to wider military situational awareness. In each case, the reporting question should be explicit, and observations should be distinguished from interpretation. An image of vehicles near a river is evidence of vehicles; it does not establish their purpose, affiliation or intended movement.

Persistence should be understood as the ability to maintain an adequate *information service*, not continuous flight by one aircraft. Sustainable surveillance is limited by maintenance cycles, personnel duty, batteries or

fuel, weather, data processing and the operator's cognitive load. The larger the volume of imagery, the greater the challenge of sorting time-sensitive observations from routine activity. Under pressure there is a tendency to replace disciplined reporting with a flood of unqualified visual material. This can reduce rather than improve decision quality.

A useful operational report therefore includes when and where the observation was obtained; whether position and time data are trusted; the sensor and visibility limitations; the analyst's confidence; and any material uncertainty. Terms such as 'possibly', 'probably' and 'confirmed' should have agreed definitions rather than reflecting personal style. Relevant negative observations should also be described carefully: failure to see something beneath foliage or in poor weather is not proof that it is absent.

The strongest Ukrainian lesson here is integration. UAS changed tactical awareness because information could influence action within organisations that were adapting their command processes. A Southeast Asian force should resist acquiring a surveillance product that cannot be shared, understood or acted upon by its intended users. The quality of the reporting chain is part of the surveillance capability and should be tested at the same standard as flight performance. [2][4]

ADG analysis | Operational implications and required proof

Surveillance should be measured as a decision-support service. Useful outputs include a verified change of infrastructure status, a time-qualified account of route condition, a properly located visual record of an area and a report of limitations requiring complementary collection. “Hours flown” or “number of videos collected” are workload indicators, not evidence that a formation improved its understanding.

The reporting discipline must survive imperfect collection. If observations are separated by an unobserved interval, the analyst should not interpolate a continuous movement story without corroborating evidence. If the origin and time of imagery are uncertain, the record should disclose that limitation rather than silently carry it into an apparently authoritative operational map. Personnel trained only to pilot a UAV will not necessarily possess the skills to assess intelligence reliability, nor should software labels displace human scrutiny.

9. Target identification and the danger of false precision

A UAS sensor can support identification of objects and movements, but an image alone is seldom sufficient to determine legal status, affiliation, intent or the wider consequences of armed action. That distinction becomes exceptionally important in the Southeast Asian environment, where civilian river traffic, agricultural vehicles, relief workers, emergency services and military users may share constrained infrastructure. Electronic interference can compromise geolocation or timestamping; canopy, buildings and weather may restrict visual context. These problems cannot be solved by declaring that a camera offers 'high definition'.

A serious doctrine must separate detection, classification, identification and authorisation. Detection establishes that something may be present. Classification proposes a type or category. Identification attributes a particular identity or status at a stated confidence. Any decision to use force requires additional command and legal judgments, including the rules governing military objectives and civilian protection. These are distinct responsibilities, even if one operator sees all of them represented on a single display. The ICRC stresses that armed drone use is governed by the same obligations of distinction, proportionality and feasible precautions as other means of warfare. [12]

As automation assists imagery analysis, commanders face an additional hazard: a graphical marker or algorithmic confidence value may appear more certain than the underlying data. A model trained on one landscape can behave differently over Southeast Asian vegetation, settlements and waterways. Training images may not adequately represent local vehicle types, clothing, vegetation or weather. Even strong object recognition would not itself establish whether a person is a combatant, has surrendered or is otherwise protected. The ICRC's October 2026 briefing on autonomous weapons highlights that context-dependent legal and humanitarian judgments cannot be reduced reliably to simple technical indicators. [13]

Accordingly, doctrine should require explicit acknowledgement when information is insufficient and prevent uncertainty being disguised by precise-looking maps or numerical scores. Video clips should retain provenance and context where practical, not merely a cropped image of the object of interest. The responsibility to question an apparently convincing product should be normalised, especially when connectivity is degraded or an observation cannot be independently corroborated.

ADG analysis | Operational implications and required proof

Target-related intelligence demands an additional safeguard. Detection means that something of interest appears to be present; classification means that the object is assigned to a category; identification entails a more demanding conclusion about what it is. A sensor observation does not establish hostile intent, civilian status or authority to use force. These are different judgments, often requiring information from outside the UAV feed. The fact that an image looks precise does not make its interpretation reliable.

For national doctrine, the important standard is a documented evidential chain, trained personnel, documented uncertainty, legal review and the capacity to decline to decide. That last capability is critical in mixed civilian environments. The UN Human Rights Monitoring Mission reported severe civilian harms associated with short-range drone attacks in frontline Ukraine, illustrating why apparent camera precision is not synonymous with lawful or responsible force application. [12][17]

10. Defensive manoeuvre in narrow corridors of movement

Roads, valleys, ridgelines, causeways and bridge approaches can channel movement in much of Southeast Asia. A national road may be the only practical heavy-vehicle connection through mountains; a raised causeway may be the only dry route across wetlands; and an urban bridge may carry military, emergency and civilian traffic simultaneously. This geography makes route-condition information unusually important. It does not imply that a commander can assume full knowledge or control of the corridor through UAS observation alone.

The potential defensive contribution of UAS lies in improving understanding of the corridor as a changing system: road usability, bridge condition, flooding, smoke, landslides, civil traffic, infrastructure damage, alternate access for emergency services and the degree to which terrain obstructs observation. Engineers, traffic-control authorities, logistics planners and manoeuvre commanders may need different information from the same survey. The drone enterprise should serve those decision-makers rather than generate a single undifferentiated video feed for all recipients.

The strongest limitation is incomplete visibility. A narrow road may seem easy to monitor from above, yet bends, embankments, settlement roofs, ravines and dense vegetation hide critical sections. Terrain that concentrates movement also concentrates civilian exposure and can obstruct communications between aircraft, ground stations and headquarters. An aircraft can create a misleading impression of coverage if its observer sees the most visually accessible segment and implicitly assumes that the unseen remainder is similar. Doctrine should require explicit coverage limitations in all reporting.

The availability of UAS can improve the tempo of route assessment, but it must not become an excuse to disregard engineering reconnaissance or ground reports. Aerial imagery can reveal an inundated bridge deck; it may not establish load-bearing safety. It can show an apparently open road; it may not identify ground instability under the pavement. During severe weather the aircraft may be unavailable at precisely the point when route conditions are changing fastest. Forces must retain non-UAS means of reporting and corroboration.

A corridor also creates competing priorities. Military formations may seek situational awareness while civil authorities maintain evacuation routes and humanitarian access. The use of UAS should not inadvertently close an airport approach, interfere with emergency helicopters or compromise rescue operations. Local airspace coordination and agreed reporting responsibilities are therefore components of defensive

effectiveness, not administrative distractions. The appropriate tactical fundamental is to preserve reliable decisions under constrained movement rather than to promise persistent observation of every metre.

ADG analysis | Operational implications and required proof

Restricted corridors in Southeast Asia are not single lines on a map. A valley route may include short bridges, culverts, steep cuttings, built-up sections, narrow settlements, landslide-prone slopes and stretches beneath tree cover. A coastal route may be constrained by tidal bridges, causeways and limited alternate roads. Even in a defensive scenario, the information need is broader than detecting vehicles: commanders need a trustworthy picture of infrastructure state, obstructions, civilian movement, weather-related deterioration and places where observation has not been possible.

Ukraine's 2023 offensive provides cautionary evidence on predictable movement and the risks created by persistent enemy surveillance; it does not provide a ready-made Southeast Asian corridor doctrine. An important inference is that a formation must understand how enemy observation interacts with its own mobility and reporting delays. The analytical conclusion is to integrate engineering, transport, weather, intelligence and civilian liaison into the same assessment process. This paper does not propose engagement geometry, route interdiction schemes or strike placement. [18]

Peacetime demonstrations often show the most convenient direction of flight and the clearest section of terrain. National testing should instead assess whether the system describes the limits of its observation and whether a commander's decision changes when those limits are disclosed. The result may be a requirement for ground verification rather than a more capable aircraft. A truly useful UAS programme must be comfortable arriving at that conclusion.

11. River defence: hydrology, observation and information continuity



Figure 3 | Tropical river environment and the challenge to achieve persistent, accurate UAS observation and reporting.

Rivers in Southeast Asia are not static lines on a military map. Flow, width, bank condition, channel position and surrounding accessibility can change materially across the monsoon cycle. Floodplain settlements may be connected by ferries and small boats, with local users possessing knowledge not represented in national mapping. Urban river sections can include bridges, culverts, industrial waterfronts and emergency-service routes; rural rivers can contain wooded islands, mangroves, inundated vegetation and highly variable bank conditions. A river-focused UAS doctrine must begin with this physical and human reality.

The most robust UAS contribution is improved awareness of current conditions. Aerial surveys can help document flooding, visible damage, debris, bridge approaches, landing-site usability and changes in civilian traffic. They can support communication between engineers, civil authorities and formation headquarters

when those parties are otherwise relying on stale maps or fragmentary reports. Periodic comparison of properly dated imagery may be more valuable than hours of uninterrupted video because it reveals that physical conditions have changed. In a flood emergency, those changes may matter to public safety as much as to military movement.

River corridors also impose severe observation limits. Canopy along banks can conceal what is happening immediately behind the vegetation; reflective water and shadow complicate interpretation; heavy rain and low cloud reduce flying opportunities; and shifting channel conditions invalidate earlier imagery. The presence of boats or other activity is not by itself evidence of hostile intent. This matters especially in commercially active waterways and settlements where military and civilian users cannot be assumed to be geographically separated.

A defensible procedure for river surveillance therefore emphasises measurement and provenance. Reports should state the time of observation, the segment actually visible, the limits of water-level interpretation and whether the report is directly observed or derived from other sources. Engineers and hydrographic authorities remain responsible for judgments that cannot be made from imagery alone. UAS can contribute to a common picture; they cannot establish bridge strength, water depth or ground bearing capacity merely by being overhead.

The broader defensive implication is one of command continuity. In a river-dominated region, disruption to one crossing or communications point can have disproportionate effects on the movement of civilians, relief supplies and military support. UAS can assist commanders in recognising the implications, but only if the information is delivered to the relevant authorities with sufficient confidence and urgency. Training should make river conditions dynamic rather than using a fixed map and a clean communications network. A credible exercise must include misleading imagery, interrupted reporting and rapidly changing weather so that uncertainty becomes visible.

ADG analysis | Operational implications and required proof

River defence is best understood as a combined hydrological, information and infrastructure problem. The operational geography of a river can change between seasons and, in extreme cases, within hours. Width, current, channel shape, tributary flow, debris, sandbars, banks, vegetation and boat traffic affect what can be seen and what a report may mean. In delta environments, settlement, fishery operations and river transport create difficult civilian-identification conditions. Across much of the Mekong system, seasonal flood pulses are a normal feature rather than a rare exception. [6]

The destruction of the Kakhovka dam on 6 June 2023 is a particularly useful warning against treating mapped water obstacles as fixed. The flood transformed the operational and civilian environment, displaced communities, affected transport and generated uncertainty across both banks. A United Nations environmental assessment documented extensive hydrological and geomorphological change. The Ukrainian case does not prove a tactical drone solution for tropical river defence; it shows that doctrine must accommodate the rapid invalidation of prior information. [20]

National riverine UAS assurance should therefore be organised around the quality and timeliness of information shared with engineers, river authorities, local administration and military command. When rain or disruption removes UAV access, field procedures need to record the last credible observation and transfer responsibility to other approved collection methods. It is inappropriate to portray a UAV as a permanent answer to the uncertainties of a river system. The river and the electromagnetic environment both remain active, changing elements of the battlespace.

12. Littoral and archipelagic implications

An island chain requires different assumptions from a continuous land frontier. Units may depend on maritime supply, separated electrical grids, infrequent technical support and communications routes crossing open water or difficult coastal topography. Weather can be localised and severe. Marine corrosion, rough handling

during transport and the availability of spare parts affect readiness even when a system is not flying. The relevant unit of analysis is therefore not the aircraft's advertised range but the reliability of the entire service delivered across dispersed operating locations.

UAS may support coastal awareness, infrastructure inspection, maritime safety observations and the transfer of selected information between isolated formations. However, a sensor that can see a vessel is not necessarily able to identify it reliably, determine its purpose or support safe action in crowded waters. Fishing activity, local transport, ferries and humanitarian movement require caution in interpretation. Existing maritime and air surveillance organisations should not be bypassed merely because the imagery comes from a low-cost aircraft. Shared definitions and clear responsibility for assessment are essential.

It is tempting to regard islands, straits and narrows as inherently favourable to uncrewed technologies because movements are geographically constrained. The same geography may instead make all sides sensitive to weather, signal obstruction and support shortages. The conclusion is not that UAS are unimportant, but that their value must be demonstrated across separate sites, seasonal conditions and communications states. The archipelago rewards robust logistics and data sharing at least as much as advanced airframes.

ADG analysis | Operational implications and required proof

Archipelagic operations magnify the difference between owning a platform and being able to sustain a service. A remote site may have a working airframe but no reliable means to deliver large imagery files, no dry storage, no qualified maintainer or insufficient spare batteries. Harsh weather may delay sea or air resupply precisely when a local commander has the greatest need for updated information. National doctrine must define what reporting quality is required from an isolated site, what level of autonomy is authorised and what data can be transmitted by limited connectivity.

A single island-based trial should not establish national suitability. Differences between coral coast, forested volcanic upland, dense settlement and exposed strait environments are substantial. Inter-service agreements should also address airspace management, sovereignty, civil aviation and emergency-response responsibilities. These institutional interfaces are as consequential as a platform's advertised range.

13. Armed and direct-attack UAS: capabilities, limitations and control

The Ukrainian war has demonstrated the operational importance of weaponised drones, including remotely piloted attack systems and one-way munitions. It has also shown that their effects cannot be assessed independently of surveillance, command authority, communications, the opposing force and the wider combined-arms situation. This paper recognises armed UAS as a distinct military capability, while deliberately excluding target-selection methods, attack profiles, employment geometry and procedures for defeating opposing defences. Its concern is the doctrine required to control such a capability responsibly and evaluate whether claimed performance is credible. [1][3][4]

Direct-attack systems raise questions that unarmed surveillance systems do not. What evidence establishes an appropriate level of control over the aircraft and weapon? How is the operator's understanding of what is being observed verified? What happens when navigation data are unreliable or a link becomes unavailable? How is authority for the use of force assigned and recorded? How are wrong-location, wrong-object and civilian-harm risks recognised? How does the organisation investigate failures and learn from them without encouraging concealment? These are military-command questions as well as technical and legal questions.

The observation that a weapon system is guided by a camera does not by itself establish precision in a legal or humanitarian sense. A clear image may omit protected persons outside its field of view. A moving object may be identifiable as a vehicle but not as a lawful military objective. A damaged or unreliable navigation system may make geolocation uncertain. Under International Humanitarian Law, an armed drone is not exempt from the duties of distinction, proportionality and precaution because it is small, inexpensive or remotely controlled. [12]

The distinction between automated flight and autonomous selection of targets must also be preserved. Automated stabilisation or navigation does not necessarily mean the system independently selects and attacks an object. Systems that do select and apply force without human intervention pose additional issues of predictability, accountability and compliance. The ICRC's 2026 publications explain the importance of meaningful human judgment and the limits of reducing protected status or civilian risk to algorithmic profiles. These issues are acute where people and vehicles move through populated routes, rivers and settlements. [13][14]

For Southeast Asian doctrine, armed-UAS development should never be assessed solely by whether a demonstration weapon reaches a test object. Acceptance must include independent legal review, command authorisation, software and data assurance, operator competence, flight and ground safety, appropriate record-keeping and the performance of fail-safe provisions in realistic environments. Procurement must budget for secure storage, maintenance, training and accountability over the entire service life. An organisation that cannot substantiate these controls has not established a mature armed-UAS capability, regardless of its technical promise.

ADG analysis | Operational implications and required proof

Armed and direct-attack UAS are an important part of contemporary conflict, and excluding them from doctrine would conceal a material capability trend. In Ukraine, uncrewed platforms have been used for reconnaissance, explosive delivery and self-destructive attack, while adversaries simultaneously developed methods to detect, disrupt and defeat them. The intensity of these uses and adaptations is well documented. What the public record does not provide is a universal set of conditions under which a particular class of aircraft reliably succeeds against a competent opponent. [1][3][24]

A defensible national treatment separates three questions. First, can the technical system be demonstrated to operate within a safe and clearly defined envelope? Second, can trained operators and commanders maintain adequate information, control and accountability when the operating environment degrades? Third, has the state established the legal, organisational and political authority for any use of force? These requirements are cumulative. A favourable result in one area cannot compensate for a failed safeguard elsewhere.

For Southeast Asian forces, dense civilian settlements, inland water transport, common agricultural infrastructure and protected locations create demanding practical constraints. The paper recommends a separate assurance and approval pathway for armed capability, with legal review, positive command responsibility, independent trials and audit records. It does not offer target-engagement sequences, improvised weapon adaptations, targeting methods or instructions to overcome defensive countermeasures. [12][13][14][17]

14. Counter-UAS, force protection and survivability

In Ukraine, the contest between UAS and counter-UAS activity has made routine movement, storage, communications and logistic functions more difficult. A Southeast Asian defence force should therefore develop UAS and counter-UAS understanding together, while preserving appropriate legal authority over any interception or electronic action. It would be a mistake to train operators to use UAS in isolation from the fact that the opposing force may use similar capabilities to observe them. [1][2][5]

This paper focuses on the protective and organisational aspects of that challenge. Bases and temporary facilities need proportionate risk assessment, alerting, incident reporting and coordination with the agencies authorised to respond to hostile aircraft. Personnel must understand the distinction between a sighting, a credible threat and verified hostile behaviour. An unfamiliar drone is not automatically a lawful target. In civilian-populated environments, indiscriminate use of countermeasures can create hazards for other aircraft, communications users and members of the public.

Protective capability should be evaluated through realistic exercises that include false alarms, multiple aircraft activity, airspace conflicts, poor weather, incomplete detection information and command disruption. The

outcome sought is not simply the detection of objects, but an accurate and timely protective decision within lawful authority. Unit preparedness depends on reporting discipline and cooperation across aviation, communications, intelligence, police and civil organisations. Where a system is authorised to interfere with an aircraft, its performance and collateral effects require separate controlled assessment.

The important tactical lesson is that the presence of an aerial threat changes the risk context of apparently routine activities. This should influence training, readiness assessment and command awareness without producing an assumption that every threat can be solved by a single electronic or physical technology. Protection requires a system, just as UAS employment requires a system.

ADG analysis | Operational implications and required proof

The presence of low-cost aircraft in the air also creates a persistent counter-UAS requirement for friendly forces. The general defensive response should be framed in terms of layered protection, public safety, aviation deconfliction, detection confidence and integration with authorised command systems. Protective methods and their effectiveness are context dependent and cannot be inferred from product demonstrations alone.

A force relying extensively on friendly UAS should test the risk that its own safety systems, electronic emitters, information practices or defensive measures make those operations less reliable. Accountability for deconfliction is consequently joint and must extend beyond the UAV specialist branch. The institutional objective is not perfect immunity but a realistic, testable description of what the force can continue doing when aircraft or links are compromised.

15. Sustainment in heat, humidity and distributed operations

The Ukrainian evidence makes clear that losses, maintenance, repair and replacement shape the effectiveness of UAS forces over time. In Southeast Asia, even a non-combat training programme must account for tropical heat, moisture, dust, mould, salt, insects, power quality, batteries and transportation between separated bases. Logistics can become more demanding when a unit is dispersed across islands or when roads are interrupted by flooding. An airframe that needs imported parts may remain unavailable for weeks despite a minor failure. [1]

A serious readiness system should distinguish the number of aircraft owned, aircraft technically serviceable, trained teams available, supported missions that can be sustained and missions actually completed to information-quality standards. A single high-performing demonstration team may conceal a force-wide shortage of batteries, maintainers or replacement sensors. The relevant question is whether the capability can be reproduced across units and maintained after the initial burst of activity.

Power supply deserves more attention than it usually receives in concept papers. Charging, transport, storage and battery-health monitoring are routine in peacetime but can become limiting factors at isolated posts and during severe weather. Records of cycle life, premature failures and field charging incidents should inform procurement and safety policy. Software support and cybersecurity are equally relevant; an otherwise flyable aircraft can be operationally unusable if its applications, credentials or data services are unavailable.

Contractual arrangements should preserve access to maintenance information, acceptable spare-part lead times, technical documentation and an exit pathway from unsupported proprietary systems. Buying a large fleet without provision for repair and replacement creates the appearance of capacity rather than assured capacity. Doctrine should treat sustainment failure as an operational learning point, not merely a technical administration problem.

ADG analysis | Operational implications and required proof

Sustainment is the test of whether a drone fleet is military equipment or a collection of demonstrations. UAS availability depends on batteries, charging, weatherproof storage, connectors, propellers, software, technical documentation, firmware governance, trained personnel and recovery from ordinary breakage. In tropical island environments, salt and persistent moisture may increase the labour burden while dispersed bases slow

component replenishment. A credible force-development estimate includes repair turnaround and crew fatigue as well as purchasing price.

A system that succeeds on day one and becomes unreliable by day five should not be reported simply as successful. Commanders need to know how much useful information was produced during repeated operations, whether the evidence trail remained intact and how maintenance affected readiness. The true cost measure is a sustained, timely, trusted intelligence output under defined conditions.

16. Command integration and the problem of information overload

UAS data create value only when they improve the decision process. A headquarters receiving many simultaneous feeds can become slower if it lacks prioritisation, trained analysts, clear ownership of assessments and disciplined reporting. The assumption that every commander should see every video stream is therefore questionable. The information requirement should determine who receives raw imagery, who receives analysed products and who receives a concise report of a material change. Raw video is not itself a common operational picture.

Command arrangements should prevent the operator, analyst and decision-maker from becoming blurred into one informal role merely because digital tools make immediate sharing possible. A pilot concentrates on safe operation and sensor tasking. An analyst evaluates what can be inferred from the material. A commander evaluates operational relevance and exercises authority. In smaller teams individuals may perform more than one role, but the responsibilities remain distinguishable and should be explicitly understood.

Information security also has practical consequences. Unrestricted use of consumer cloud services, personal devices or poorly managed data repositories can produce privacy and security risks. A national UAS programme should set data-retention standards, access controls, evidentiary handling rules and arrangements for sharing with other services. This is particularly important where imagery includes civilians, private property or sensitive infrastructure. Information should be available to authorised users without becoming indiscriminately accessible.

A commander should be able to ask five questions of any significant UAS report: What was observed? When and where was it observed? What are the material limits of the sensor and data? How certain is the assessment? What decision does it inform? If the team cannot answer those questions, additional video bandwidth or aircraft numbers are unlikely to cure the underlying problem. In degraded communications conditions, the answers may be partial; reporting that fact is a mark of professional competence rather than weakness.

17. Training: moving beyond peacetime proficiency

A peacetime qualification generally proves that an individual can prepare and operate an aircraft under authorised conditions. It does not establish that the team can provide dependable information while tired, wet, isolated, electronically disrupted, under simulated opposing pressure or short of spare parts. This distinction should sit at the centre of Southeast Asian doctrine. The training progression must preserve baseline aviation safety while introducing conditions that test the wider system rather than simply making flying more difficult.

The first layer is basic professional competency: aircraft safety, legal responsibilities, meteorology, maintenance, human factors, airspace coordination, incident reporting and responsible handling of information.

The second is mission competency: expressing an information requirement, managing sensor limitations, documenting observation quality and delivering the result to the appropriate authority.

The third is environmental competency: conducting authorised operations amid seasonal rain, heat, coastal exposure, forest and urban clutter, with conservative safety thresholds and documented reasons for cancellation.

The fourth is disrupted-system competency: identifying failures or inconsistent information, maintaining safety, reporting uncertainty and switching to authorised non-UAS processes when the system cannot deliver its intended product.

A fifth layer should test integration across the formation. UAS teams, engineers, communications specialists, logisticians, aviation authorities, analysts and commanders should participate in the same scenario. A simulated flood on a major road might require the UAS team to provide visual observations, the engineer to determine whether more evidence is required, the headquarters to update a route status and the civil authority to receive an appropriate safety notification. The value lies in the integrity of the full reporting and decision chain. A successful sortie that produces no usable decision support should be scored accordingly.

Red-team activity should be authorised and safely controlled, with emphasis on realistic uncertainty, interruptions, false reports, conflicting indications and practical system failures. Exercises do not require uncontrolled interference with public spectrum or civilian aircraft. Simulated disruption, closed-range testing and controlled laboratory assessment can provide meaningful evidence without compromising public safety. Where live EW testing is appropriate, it must follow national legal, technical and range-safety requirements. The training objective is to understand capability boundaries, not to reward risk-taking for its own sake.

Instructors should be selected for teaching ability, technical currency and experience in realistic environments, rather than relying solely on impressive combat narratives or racing skills. Combat-experienced Ukrainian practitioners can provide valuable insight into adaptation, operator workload, failure reporting, contested communications and the difference between observed effects and assumptions. Their experience should be integrated with local meteorologists, engineers, legal advisers, airspace authorities and experienced Southeast Asian field personnel. Combat lessons imported without local validation risk becoming misleading.

An institutional learning cycle should follow each substantive exercise. Deficiencies should be recorded with evidence; technical problems distinguished from command or training problems; corrective action assigned; and retesting scheduled. Video highlights and anecdotal feedback have a role, but they are insufficient evidence for doctrine. The most mature formation is not the one that reports few failures; it is the one that identifies failure mechanisms early and changes its practice quickly.

ADG analysis | Operational implications and required proof

The central training error is to create highly competent pilots while leaving commanders, information analysts, maintainers, communications specialists and legal advisers effectively untrained in the full process. Ukrainian experience suggests that learning should be organised around the whole unit and its adaptation cycle. A good syllabus progresses from technical competence to collaborative reporting, safety and information validation, then collective exercises under realistic constraints. The final assessment is the supported command decision, not an aerobatic display.

Exercises should include adverse-weather postponement, unexpected absence of a key specialist, failed power provision, non-available network services, unverified reports, civilian-movement ambiguity and a superior headquarters demanding answers before the evidence is ready. Such training is more intellectually and organisationally demanding than straightforward flight proficiency. It also generates the facts from which local SOPs can be revised.

18. An evidence-led validation programme for Southeast Asia

FIGURE 4 | THE READINESS TEST: AVAILABLE AIRCRAFT ARE NOT EQUAL TO USABLE INFORMATION



FIGURE 4 | Readiness is the sustained output of an entire organisation.

A national or service-wide test programme should begin with representative mission statements rather than brand selection. These could include routine terrain assessment, river-level and infrastructure observation, coastal facility monitoring, emergency communications reporting and delivery of appropriately qualified situational information to headquarters. Each task should specify who needs the information, the decision it informs and the threshold beyond which the resulting evidence is no longer useful. Armed-system testing, where authorised, requires a distinct governance and safety programme.

The programme should establish a baseline in controlled conditions, then assess environmental stress, communications degradation, organisational integration and sustainment over time. These are categories of evidence, not a sequence for combat employment. Environmental stress should cover representative tropical heat, humidity, rainfall and terrain while maintaining aviation safety. Communications tests should distinguish aircraft control, payload information and operational distribution, and document the effects of disconnection or doubtful navigation information. Organisational tests should measure whether the information reaches the designated decision-maker in a useful form. Sustainment tests should measure the capacity to reproduce performance after repeated use.

Measurements must include failures and no-go decisions. A safety-conscious cancellation in dangerous weather may demonstrate effective command judgment. An image that is insufficient for object identification should be recorded as insufficient, not upgraded into a success because the aircraft returned. A test must also distinguish between observed values and estimated values; nominal manufacturer specifications should not enter the evidence register as though they were field results.

The following dimensions form a practical basis for acceptance evidence: safe aircraft control; information timeliness; geospatial and time integrity; analyst confidence; interoperability; weather and terrain limits; training burden; maintainer workload; logistic demand; data security; and recovery from interrupted service. The thresholds selected will differ by mission and national requirements. A single pass/fail score cannot adequately represent this multidimensional capability.

Testing should use locations representative of national terrain without assuming that one locality proves suitability for the whole archipelago. For an Indonesia-like state, at minimum the evidence base should account for upland forest, lowland river or plantation conditions, a built-up corridor, a coastal site and a dispersed island support environment. The programme must not assume that a trial conducted in open fields

near a capital city establishes capability in eastern island terrain or a forested border region. Comparable cross-season evidence is necessary wherever seasonal changes could materially alter performance.

Independent observers and records should support the programme. Industry representatives may assist with equipment setup and diagnosis but should not be solely responsible for defining success. Personnel responsible for communications, aviation safety, data assurance and operational analysis should review results together. The output should be an auditable statement: what the system demonstrated, under which conditions, with what personnel and support, against which information requirements, and with which unresolved limitations. This is the foundation on which a credible tactical manual can be written.

ADG analysis | Operational implications and required proof

A national trial must publish its acceptance conditions before conducting the demonstration. Evaluators should know which operational information requirement is being tested, which locations and seasons are representative, which safety constraints govern the work and who will determine whether results are sufficient. Trials should distinguish repeatability from isolated success. Where results are mixed, the record should say so rather than collapsing the outcome into a single overall score.

The report should include common observation and reporting errors, source-data integrity, image timeliness, missed or ambiguous observations, interruptions, equipment downtime, personnel work rates and uncertainty in the conclusions. Opposing conditions may be represented through authorised exercise injects and independent evaluators. Trials that require spectrum activity must be managed by competent national authorities, not improvised by instructors.

There should be a clear institutional decision at the end of every trial: evidence accepted for a specified mission, further limited testing required, or capability not demonstrated. Procurement and doctrine approval should depend on that decision. A permanent lessons team should record which conclusions remain provisional and which have been independently replicated.

19. Illustrative Southeast Asian exercise vignettes

Vignette A: Rain-affected mountain corridor

A fictional territorial formation is asked to provide an updated condition report on a road linking two settlements through steep forested terrain after several days of intense rain. The exercise includes poor satellite-navigation confidence, variable radio coverage, continuing civilian use of the route and uncertainty about a bridge approach. The UAS team obtains partial imagery but cannot reliably observe several sheltered bends. A second report is delayed before reaching the route authority. The decisive test is not whether the aircraft completed its planned circuit; it is whether the command system recognises the limits of coverage, preserves the distinction between observed and inferred road conditions and avoids issuing an overconfident route-clearance statement.

The training assessment should examine the accuracy of timestamps, identification of unseen areas, the handling of inconsistent position data and the timeliness of the information received by the engineer and headquarters. The exercise succeeds if the organisation reaches a justified decision and clearly states where further evidence is needed. It fails if attractive aerial footage is treated as complete knowledge of the corridor.

Vignette B: Monsoon river and mixed civilian traffic

A second fictional formation is tasked with supporting a river-condition assessment during a changing flood situation. Ferry traffic, fishing boats, temporary structures, debris and rising water complicate the scene. Unreliable communications interrupt the transfer of some imagery, and weather causes a conservative suspension of flying. The exercise tests whether the team can report the last reliable observation, clearly identify the period for which conditions are unknown and coordinate with hydrographic, engineering and civil authorities. It also tests whether commanders can continue making proportionate decisions without assuming that the river is fully observable.

The lesson is not a particular deployment technique. It is the need for a river doctrine that incorporates civilian activity, hydrological uncertainty, mixed information sources and safe alternatives when UAS become unavailable. A good report may say that the available evidence is insufficient to approve a movement or infrastructure decision. That is a positive professional outcome.

Vignette C: Dispersed islands and a disrupted reporting chain

A third exercise involves a coastal headquarters and several remote sites, each with differing power availability, maintenance capacity and weather. All sites possess aircraft, but one cannot transmit high-bandwidth imagery, another has an equipment fault and a third loses access to an expected support delivery. The headquarters must obtain current infrastructure status reports and distinguish fresh observations from older imagery. Evaluation focuses on standard reporting, shared information definitions, record integrity and sustainable support—not on the total number of nominally assigned UAVs.

Across all three vignettes the intended lesson is identical: the operational product is reliable, contextualised information and properly exercised command judgment. The aircraft is an enabling component, not the definition of success.

20. Force design, procurement and institutional governance

The central procurement risk is to buy hardware before defining the service it must provide. An effective force-development programme begins with mission requirements, an inventory of terrain types, communications constraints and trained personnel, and a realistic estimate of maintenance and replacement capacity. Purchases should be assessed against interoperability, security, availability of technical documentation, sensor evidence, support burden and the ability to adapt as technology and threats change. A nominally inexpensive fleet can become costly if it requires incompatible applications, dedicated consumables and separate training ecosystems.

Force design should distinguish what must be common across the military from what must vary locally. Common standards should cover safety, incident reporting, data fields, classification of observation confidence, training progression, legal responsibility and arrangements for inter-service coordination. Different regions or formations may need different platforms and sensors. Standardisation should enable information and support interoperability without forcing a single aircraft to fulfil dissimilar missions. The Ukrainian move from a fragmented collection of improvised systems toward more formal specialisation offers a relevant institutional lesson. [1]

Governance must be capable of revising its own assumptions. A standing lessons function should review verified foreign evidence, national test results and significant incidents. Changes should be incorporated into training and equipment requirements through a documented process. Legal advisers, communications specialists and aviation authorities should have an assured place in capability review. For armed systems, the required decision authorities and safeguards are additional and cannot simply be appended to an unarmed drone procedure.

Operational confidence should be reported in plain language. For example, a force might state that it has demonstrated effective infrastructure-surveillance reporting in dry-season lowland conditions but lacks evidence for sustained monsoon use and contested GNSS. Such a statement is more useful to a defence leadership than an undifferentiated claim that a unit is 'UAS operational'. Mature doctrine defines the boundary of knowledge as clearly as the demonstrated competence.

ADG analysis | Operational implications and required proof

The national benefit of Ukrainian expertise lies particularly in challenging inherited assumptions. Veterans of the full-scale war can explain which procedures were overtaken by enemy adaptation, where a seemingly effective technology failed at scale and why the operational burden shifted between pilots, analysts, maintainers and command posts. Such experience should be captured systematically and assessed with

documentary evidence. A celebrated anecdote is a prompt for investigation, not in itself a validated requirement.

In procurement, credible independence requires that the people defining operational requirements are not solely those selling a specific system. National armed forces should retain ownership of testing criteria, data, cyber-security requirements, audit access and decisions to adopt equipment. Ukrainian experts can contribute critically without displacing national decision-making.

21. Proposed foundational principles for doctrine

Principle 1 — Mission first. Define the decision and information requirement before selecting the aircraft, sensor or communications service. A flight that does not answer the relevant question is not a successful mission merely because it occurred.

Principle 2 — Separate the system's links. Aircraft control, payload-data transmission and delivery of assessed information are different functions with different failure modes. All three must be considered in readiness assessment.

Principle 3 — Treat disruption as normal. Enemy activity, own-force interference, terrain and weather can degrade communications and navigation. Training and reporting must acknowledge the resulting uncertainty rather than presuming continuity.

Principle 4 — Do not confuse observation with knowledge. Detection does not equal classification; classification does not equal identification; and neither imagery nor an algorithmic label independently authorises a military action.

Principle 5 — Preserve command accountability. Remote operation does not dilute responsibility for aviation safety, use of force, information quality, legal compliance or civilian protection. Armed systems require distinct governance and evidence.

Principle 6 — Design for the local environment. Tropical forests, river floodplains, highland corridors, cities and islands require different performance evidence. Foreign combat experience should initiate local testing, not replace it.

Principle 7 — Measure the sustained service. Evaluate useful information delivered over time, not simply airframes purchased, flying hours or impressive images. Maintenance, power, personnel and data processing are part of the capability.

Principle 8 — Learn faster than procedures become obsolete. Publicly documented Ukrainian experience is evidence of constant adaptation. The national institution must maintain a disciplined cycle of testing, reporting, correction and revalidation.

22. Why Ukrainian operational expertise matters

The case for a structured Ukrainian advisory contribution is strong, provided the purpose is correctly defined. The purpose is not to import a Ukrainian battlefield method wholesale, nor to stage a demonstration of the latest aircraft. It is to make available the judgement of personnel who have spent years confronting an opponent capable of observing, interrupting, adapting and inflicting losses. Those experiences are valuable because they include failure, improvisation, equipment limitations, human error and the consequences of relying upon information that was late or wrong. A military organisation with no comparable contemporary combat record cannot easily reproduce that experience through peacetime exercises alone.

The full-scale invasion of Ukraine began in February 2022; by November 2026 the conflict offers approximately four years and eight months of intense contemporary experience, built on Ukraine's earlier conflict experience since 2014. That record spans a transition from improvised civilian-adapted UAV use to an extensive, specialised and contested UAS ecosystem. However, experience is not uniform. A specialist whose expertise is in an open agricultural front, winter operating conditions or a particular system class will not automatically

be an authority on tropical hills, coastlines, mangroves or archipelagic communications. The value of a Ukrainian expert is greatest when that individual's experience is clearly documented and matched to a question under examination. [1][2][3]

Ukraine's war has also been a learning contest, not a catalogue of permanent solutions. Systems that worked in one season became vulnerable in another; losses forced changes to support models and training; and short-cycle adaptation became a governing requirement. A useful expert therefore explains the context, the triggering failure, the response, the subsequent enemy adaptation and the evidence for a changed practice. This process-based understanding can materially improve a national defence force's ability to identify its own weak assumptions.

The NATO–Ukraine Joint Analysis, Training and Education Centre, inaugurated in February 2025, demonstrates that the systematic collection and institutional use of Ukrainian lessons is a recognised defence-development practice. Its existence is not an endorsement of any proposed ADG programme or a claim that NATO will participate. It is a precedent for a structured approach in which operational knowledge is assessed, translated into training and doctrine, and institutionalised through national or alliance authorities. [25][26]

22.1 The expertise required is multidisciplinary

Ukrainian contribution should be drawn from more than UAV pilots. An effective advisory group would include practitioners with recent experience in UAS mission command and intelligence reporting, electronic-warfare and communications assurance, technical maintenance and sustainment, training and force adaptation, and legally accountable operational governance. For an exercise focused on river defence or restricted terrain, engineers and reconnaissance specialists should be included in the discussion. The design should allow candid accounts of failure, not only selected success stories.

National defence representatives must be equally broad. Territorial and field forces, joint communications staff, intelligence and imagery specialists, airspace authorities, river engineers, civilian-protection/legal advisers, military education institutions and procurement staff have different and complementary responsibilities. The advisory process succeeds when they jointly develop a nationally usable doctrine—not when an external instructor delivers a stand-alone training course and departs.

All proposed engagements require host-state sponsorship, lawful approvals, security screening, applicable export-control and information-sharing decisions, and an agreed boundary between unclassified instructional material and protected operational knowledge. It should be assumed that many genuine combat lessons cannot be disclosed publicly or transferred. A professional programme values this limitation as a condition of credibility.

23. Translating combat lessons into sovereign national doctrine



FIGURE 4 | Evidence-to-doctrine conversion requires interpretation, local testing and national approval.

A country must define the defence problem before introducing external specialists. A mainland state confronting highland corridors, major rivers and cross-border population movement will need a different evidence package from an archipelagic state concerned with separated island formations and dispersed infrastructure. A country with mature encrypted military networks also faces a different starting point from a force that relies on commercial connectivity for routine exercises. Doctrine must reflect these realities, as well as the national chain of command, service responsibilities, civil aviation regime, laws governing the use of force and existing tactical traditions.

The recommended doctrinal architecture has three tiers. The national or joint tier establishes policy, command accountability, information standards, spectrum governance, airspace coordination, legal obligations and interoperability. The service or formation tier sets mission categories, training and readiness responsibilities, reporting relationships and sustainment requirements. The unit tier contains approved procedures, equipment checks, record-keeping, incident handling and local tasking arrangements. The tiers should be mutually consistent without forcing technical details into high-level policy documents.

National authorities should distinguish doctrine, tactics, techniques and procedures, and standard operating procedures (SOPs). Doctrine expresses enduring principles and responsibilities; operational concepts describe intended employment at a higher level; tactics and techniques require nationally authorised military validation; SOPs establish repeatable institutional processes. The proposed foreign advisory input can assist all levels through evidence and training review, but legal authority and final approval always remain with the sovereign force.

The validation ladder should be deliberately conservative. A Ukrainian observation becomes a documented finding only if its source and context can be adequately described. It becomes a regional hypothesis when a plausible Southeast Asian analogue is articulated. It becomes a national training or procurement requirement only after the host force tests the proposition under locally meaningful conditions. It becomes approved doctrine or an SOP only after the designated authority reviews the evidence, risk and implications. The process should remain reversible because technology, opponents and national requirements change.

23.1 Country-specific requirements analysis

The first product should be a National UAS Operating Environment and Capability Baseline. This would identify the country's relevant terrain families, seasons, road and river networks, dispersed sites, aviation regulations, communications architecture, equipment fleets, specialist workforce, training systems and maintenance capacity. It should include a candid review of electronic-warfare assumptions, including whether the force has

tested its equipment against representative controlled interference or whether it is describing a capability that has only ever operated in a benign radio environment.

The baseline must also describe authority to collect, retain, share and act on imagery. National military intelligence procedures cannot be separated from privacy, data security, civilian protection and the law of armed conflict. In several Southeast Asian environments, military and civilian traffic intermingle on the same bridges, rivers and roads. Doctrine which assumes that all moving objects in a zone are military would be both analytically unsound and legally unsafe. [12][17][23]

23.2 A doctrine board rather than a vendor workshop

The recommended mechanism is a host-state doctrine steering board. Its chair and decision authority should be national. Ukrainian practitioners would provide structured testimony, challenge assumptions and participate in evaluation. ADG Consult NZ could act, if engaged, as an independent programme coordinator, research and drafting partner, and facilitator of the evidence review. Equipment suppliers could submit data and provide support in technical trials, but should not independently certify operational effectiveness. A national legal adviser and independent safety authority should be present at key review points.

The board should own a version-controlled issue register. Each entry would record the operational problem, the proposed lesson, source confidence, expected applicability, trial evidence, unresolved risks, drafting consequence, approving official and review date. This makes doctrine a maintained institutional product rather than a one-time publication.

24. Proposed ADG Consult NZ–Ukrainian expert advisory programme

This section is a proposed engagement model, the model is designed for country-by-country adaptation and a national defence sponsor. Its strategic objective would be to use real combat experience to accelerate competent, realistic and sovereign development of UAS doctrine and SOPs. The measure of success would be demonstrably improved national decision-making, training and readiness, not the number of students exposed to an impressive equipment demonstration.

Phase 1 — Strategic scoping and authority. The sponsor identifies mission priorities, key services, legal scope, sites and personnel. ADG and national staff agree on the evidence boundary, confidentiality and reporting format. The product is an endorsed project charter and problem statement. The first milestone is a clear agreement on what the programme will and will not attempt to validate.

Phase 2 — Structured Ukrainian lessons capture. Selected practitioners participate in recorded, consented and securely handled discussions organised around specific operational episodes. Interviewers establish dates, conditions, original task, observed friction, failed assumptions, adaptive response, later counter-adaptation and limitations of recollection. Where the account cannot be independently checked, the report labels it testimony rather than verified fact. The product is a controlled lessons register, accompanied by non-sensitive teaching cases.

Phase 3 — National terrain and system baseline. Joint teams review available equipment, service networks, training, weather and geographic constraints. The process considers at least one restricted land corridor, one riverine or delta environment, an urban or mixed-settlement setting and a relevant coastal or island case where applicable. The output is a set of nationally prioritised hypotheses and preliminary acceptance criteria. The baseline should be performed before any decision to purchase or expand a particular platform family.

Phase 4 — Exercise design and supervised validation. National military exercise authorities design safe, lawful and realistic scenarios. Ukrainian advisers help construct adverse-condition injects based on documented failure modes, while local technical staff and independent observers assess performance. No exercise is considered proof of electronic-warfare survivability unless its authorised test conditions credibly represent the intended claim. The output is an evidence report, including unsuccessful tests and confidence limits.

Phase 5 — Doctrine, SOP and training development. National authors translate the validated results into a joint doctrinal outline, service supplements, SOP catalogue, instructor notes, qualification criteria and

readiness assessments. Ukrainian experts review realism; legal and aviation authorities review compliance; formation commanders assess relevance. The sponsor approves the products through its own governance process.

Phase 6 — Train-the-trainer and periodic refresh. The programme ends with national instructors able to administer exercises, record lessons, propose amendments and sustain the process. A post-trial review cycle at six or twelve months, subject to the sponsor's preferences, can capture new Ukrainian developments and national test evidence. Any continued foreign support should reinforce national ownership rather than create dependence.

24.1 Proposed expert roles and governance

Role / workstream	Contribution	National acceptance test
National sponsor / doctrine board	Owns requirements, authorities, classification and final approval.	Approvals and responsibilities documented.
Ukrainian UAS practitioners	Provide contextual combat lessons, including failure and adaptation.	Accounts source-graded; scope of expertise declared.
Ukrainian communications / EW advisers	Review realistic assumptions about link degradation and own-force interference.	Safe test design; no unsupported resilience claims.
National joint staff and formations	Define mission requirements, terrain, command and support limitations.	Use by an actual national training or doctrine system.
National engineers, intelligence and legal staff	Validate river/route observations, information standards and legal safeguards.	Cross-functional review of draft procedures.
ADG Consult NZ, if commissioned	Programme design, analytical integration, reporting and facilitation.	Timely, auditable products without vendor dependency.

24.2 What should not be promised

No credible consultant should guarantee that Ukrainian systems or methods will defeat an unspecified future adversary. Neither should a programme claim to deliver “combat proven” Southeast Asian doctrine merely because Ukrainian veterans participate. Experience can expose better questions, reveal avoidable mistakes and improve the design of tests. Only host-state exercises and evidence can establish whether a particular organisation has become competent under its own conditions. Guarantees of EW immunity, persistent tropical air coverage or a decisive contribution from armed UAS would be unsupported without a defined threat and extensive evidence.

Professional safeguards must address confidentiality, private-company conflicts, human rights, data protection, controlled military technology and the treatment of battlefield imagery. No collection or transfer of protected tactical information should be assumed. The programme should remain usable as an unclassified study and capability-development initiative even where detailed technical access is not authorised.

25. National SOP architecture and command-assurance standards

A mature SOP portfolio should be organised by responsibility and verified process, not simply by model of aircraft. Hardware-specific checklists may be necessary, but the enduring national standard concerns flight authorisation, safe operation, information integrity, accountable dissemination, incident response and maintenance records. The national baseline should specify who has authority to task the system, who may operate it, who assesses imagery, who may disseminate classified or sensitive products, and who is responsible for acting upon the information.

A core reporting standard should require a clear observation time; asset or sensor identifier; source type; geographic or position-confidence description; conditions limiting observation; degree of interpretation; whether human review occurred; origin and handling of raw imagery; and the time and recipient of each issued report. Where critical data are missing, the report should make that visible. This is not bureaucratic overhead: it prevents a plausible image from acquiring false certainty as it passes between organisations.

Communication-related SOPs should distinguish the loss or degradation of the aircraft-control function, the payload-data function and the command-reporting function. Their objective is safe, predictable organisational conduct and transparent reporting when information becomes unavailable. Detailed technical link settings, defeat methods, tactical recovery procedures and signal-countermeasure details belong in restricted, nationally authorised technical documentation, not in a public discussion paper.

For armed systems, national doctrine requires a separate governance pathway encompassing lawful authority, independent technical and safety assurance, appropriate human decision-making, documentation of distinction and precautions, accountability, and protection of civilians. A decision not to act because information is inadequate must be a recognised professional outcome. This is particularly important in riverine settlements, plantations and shared transport corridors, where civilian and military movement may be difficult to distinguish. [12][13][14][17]

25.1 Suggested SOP package

SOP family	Minimum content at public-doctrine level	Review owner
01 Mission request and authorisation	Information need; approving authority; safety conditions; record of tasking.	Operations and aviation authority
02 Flight and ground safety	Crew qualifications; airspace and weather authorisation; emergency responsibilities.	Aviation safety
03 Information capture and metadata	Time, source, confidence, missing coverage, storage integrity.	Intelligence / data assurance
04 Communications incident reporting	Loss/degradation classification; incident time; notifications and evidence preservation.	Signals / spectrum manager
05 Sensor assessment	Detection/classification/identification distinction; analyst qualifications and review.	Intelligence / training
06 Joint dissemination	Acknowledged reporting, version control and retraction/correction of reports.	Joint operations
07 River and corridor assessments	Hydrological/engineer interface; civilian infrastructure; stale-information controls.	Engineers and operations
08 Maintenance and sustainment	Serviceability, repairs, spares, batteries, power, periodic inspections.	Logistics / engineering
09 Armed-system authorisation	Legal controls, responsible command, incident records, civilian harm mitigation.	Command and legal authority
10 Lessons and change control	After-action review, discrepancy register, validation, controlled amendments.	Doctrine and lessons centre

26. Standards for validation and national capability maturity

Institutional readiness should be reported on a staged basis. A unit that has trained pilots but not demonstrated reliable information output should not be labelled fully operational. A qualification framework can recognise technical and safety proficiency, collective reporting competence, service sustainment and maturity under authorised adverse-condition testing as different achievements. That distinction provides senior decision-makers with a realistic view of limitations and of what investment is still required.

The proposed maturity framework has four descriptive states. “Introduced” means the equipment is present and the organisation has initial safe-operating competence. “Integrated” means that reports and tasking can be processed within an approved national command structure under ordinary conditions. “Validated” means that a representative unit has completed repeatable, independently observed trials for specific terrain, weather and communication scenarios. “Sustained” means the service can be reliably repeated over an operationally meaningful period with personnel, maintenance, power and reporting support. These are suggested analytical labels rather than claimed universal standards.

A favourable judgement in one terrain family must not be generalised to another without evidence. For example, an organisation may be validated for an open coastal facility assessment but still only introduced in highland jungle. It may have a useful surveillance capability but lack the legal, technical or command

assurance necessary for armed employment. The readiness declaration should state that distinction rather than conceal it behind a single aggregate rating.

The programme's results should be independent, recorded, repeatable and reviewed when new evidence emerges. This requires access to raw trial logs where lawful, consistent definitions of failure, documented safety decisions, external observation of critical assessments and a route for correcting published SOPs. Treating uncomfortable findings as valuable is the defining feature of a serious national programme.

26.1 Suggested performance evidence

Assessment dimension	Evidence that should be retained
Information relevance	Did the output answer the authorised information requirement?
Timeliness and currency	Capture, interpretation, receipt and acknowledgement times.
Accuracy and uncertainty	Ground-truth comparison; false-positive and omission records; confidence grades.
Communications assurance	Control, payload and reporting interruptions as separate events.
Environment	Weather, terrain, river state, visibility and infrastructure conditions.
Personnel	Qualifications, workload, independent observation and operator/analyst errors.
Sustainment	Availability across repeated days, faults, maintenance and support delays.
Command/legal assurance	Approval record, exercise risk decisions and treatment of ambiguous civilian activity.

27. Recommended implementation roadmap

The approach should begin with a limited, auditable national pilot rather than a force-wide equipment initiative. A realistic first engagement would establish the host's doctrine board, consult Ukrainian practitioners, capture a bounded set of documented lessons and choose several representative environmental tests. The pilot would produce a national gap assessment, an initial SOP structure and a report on what additional evidence is required. Expansion should depend on the quality of those findings.

Over the next stage, the sponsoring defence force could assign a permanent national lessons function, establish cross-service curriculum, extend representative terrain trials and build its own instructor capability. Only after the organisation has demonstrated sustained information reliability and governance should it expand mission categories or declare more demanding readiness levels. The tempo of implementation is a host-state decision, dependent on budgets, training access, systems and legal authority; an illustrative calendar cannot stand in for a national plan.

The high-value early deliverables are specific: an assessed current-capability baseline; source-graded Ukraine lessons register; country terrain and communications exposure matrix; doctrine outline and SOP portfolio; safe exercise plan; pilot evaluation report; and a train-the-trainer programme. These tangible outputs allow a defence ministry to decide whether further investment is justified and where it should be directed.

ADG Consult NZ's proposed contribution would be analytical and institutional: convene appropriate subject-matter expertise when legally available, translate evidence into national decision requirements, coordinate authorship and independent review, and ensure that the final products remain owned, maintainable and usable by the host defence force. The value proposition is stronger doctrine and more realistic training, not a claim of exclusive knowledge or vendor-linked technology.

28. Conclusions and recommended direction

The decisive lesson of Ukraine is that uncrewed systems have become embedded in modern conflict while simultaneously becoming vulnerable to sustained enemy adaptation. The availability of inexpensive aircraft can change observation and armed-effect possibilities; it cannot remove terrain, weather, logistics, communications failure, command friction or the requirement for lawful decisions. A single successful demonstration is therefore not an adequate basis for national military doctrine. The object of development

must be a whole-of-system capability supported by reliable information, trained personnel, competent maintenance, defined authority and repeatable performance under adverse conditions.

Southeast Asia requires its own doctrine. Narrow routes, steep uplands, dense canopy, deltas, monsoon flooding, mixed civilian movement, separated islands and highly variable communications environments create combinations of friction that differ from the Ukrainian front. The first obligation of the host force is to understand and test these conditions rather than assume that a European battlefield solution can simply be transferred. Evidence should be collected honestly, including negative outcomes and uncertainty about the electromagnetic threat.

The engagement of qualified Ukrainian practitioners would offer an unusually valuable source of operational judgement, particularly concerning the limits of peacetime assumptions and the pace of wartime adaptation. That opportunity should be exploited through a structured, nationally governed lessons programme. Experienced Ukrainian specialists can help identify credible problems, explain the context of past decisions and improve training realism; they cannot by themselves prove that any Southeast Asian system will survive future conflict. National doctrine and SOPs should emerge through joint analysis, local validation and sovereign approval.

The recommended direction is consequently clear: establish a national joint UAS doctrine and lessons board; capture Ukrainian experience systematically; test communications, information quality and sustainment in representative tropical conditions; develop common reporting, safety and command standards; retain a separate legal assurance process for armed systems; and institutionalise rapid review. ADG Consult NZ proposes this as a disciplined, evidence-based pathway for defence forces seeking realistic capability, credible readiness declarations and responsible use of UAS in the Southeast Asian battlespace.



ANNEX A | DOCUMENTED UKRAINE VIGNETTES AND LESSONS LEARNT

This annex is the paper's principal operational evidence annex. Each vignette concerns an actual documented event or operational episode. “Observed” identifies information supported by the cited public source; “Reported” identifies an attributed account; “Inference” identifies ADG analysis; and “National test question” identifies a matter that cannot be settled by Ukrainian evidence alone. The distinction is central: neither a press narrative nor a general pattern should be presented as independently verified tactical fact.

The vignettes are designed to support structured practitioner interviews, doctrinal debate and the planning of safe national training. They do not provide target-engagement recipes, anti-jamming settings or battlefield positioning instructions. The lessons highlight the reliability of information and institutional adaptation under pressure.

A1. Northern approaches to Kyiv: Aerorozvidka and the early invasion

LOCATION / PERIOD Ivankiv / Kyiv region | February–March 2022 • EVIDENCE: attributed contemporary account

Documented episode

During the opening weeks of Russia's full-scale invasion, Ukrainian drone operators associated with Aerorozvidka reported using small reconnaissance aircraft and other improvised technologies to observe Russian movements on the northern approaches to Kyiv. A 28 March 2022 Guardian report drew on a Ukrainian commander's account of the group's contribution to disruptive operations near Ivankiv and wider defence of the capital. The account is an example of unusually rapid adaptation by a small technical community in a high-stakes defensive campaign; its most dramatic claims require attribution rather than presentation as independently verified outcome. [22]

What the source supports — and does not prove

The contemporary reporting supports the existence and role of an adaptive UAV-capable group, the use of remotely collected information, and significant procurement and supply difficulties. It reports the commander's view of the unit's contribution to the disruption of movement. It does not establish that the unit alone stopped the northern advance, that every claimed engagement occurred as described, or that the reported effect would recur against a different force. The larger Russian failure near Kyiv had multiple military and logistical causes. [2][22]

Lesson learnt

Innovation may emerge outside formal procurement channels, but sustaining it demands compatible command relationships, lawful authority, logistical access and integration into the larger force. The relevant enduring lesson is not a particular improvisation; it is that relatively inexpensive observation becomes useful only when the receiving military organisation can interpret and use it, and when the support system survives rapid operational demand.

Southeast Asian relevance and limits

A tropical highland or restricted-road defender may encounter similar demand for timely route intelligence, but vegetation, rain, settlement patterns and different opponent capabilities make direct emulation unsound. Modern national procedures should avoid depending on ad hoc personal connections for vital spare parts or protected information distribution.

National validation question

Could a representative national reconnaissance team produce independently verified route-status intelligence, accurately mark unseen sectors and deliver it reliably to a designated headquarters over a sustained exercise?

Principal references: [22]; context [2]

A2. Ukraine's 2023 southern offensive: exposure on predictable axes

LOCATION / PERIOD Zaporizhzhia / southern front | June–autumn 2023 • EVIDENCE: field-research synthesis

Documented episode

The Ukrainian southern offensive of 2023 was conducted against prepared Russian defences with extensive surveillance, obstacles, artillery, and electronic-warfare capability. RUSI's subsequent field-based analysis concluded that persistent enemy observation placed movement on predictable approaches at substantial risk and that gaps in counter-reconnaissance, electronic protection, combined training, sustainment and engineering support contributed to the campaign's difficulties. It highlighted the vulnerability of lines of communication and the challenges imposed by obstacle and wet-gap requirements. [18][19]

What the source supports — and does not prove

This is a documented operational episode supported by analytical work using Ukrainian field experience. It is not a single independently observed drone engagement or a simple claim that UAS caused the campaign's outcome. RUSI identifies multiple interacting contributors, including force preparation and campaign decisions. Its findings support a combined-systems analysis rather than drone determinism.

Lesson learnt

Persistent observation can turn ostensibly routine movement and sustainment into major operational vulnerabilities. The doctrinal response is joint planning, counter-observation awareness, training and realistic appreciation of movement and support constraints. Communications and electronic protection cannot be delegated solely to a specialist UAV team, because the effectiveness of the whole formation is involved.

Southeast Asian relevance and limits

Constrained roads, bridges, causeways and valley routes in Southeast Asia may amplify dependence on a limited number of connections. The nature of the risk is transferable; the specific duration of exposure, equipment losses, countermeasures and tactical geometry are not. National authorities must evaluate the resilience of their own movement information and infrastructure reporting without assuming Ukrainian geography is representative.

National validation question

Does a joint formation accurately identify when its own observation is incomplete, when reports are stale and when physical infrastructure prevents an assumed movement or sustainment task?

Principal references: [18][19]

A3. Kakhovka dam breach: the river changes the mission

LOCATION / PERIOD Southern Ukraine / Dnipro River | 6 June 2023 and aftermath • EVIDENCE: UN-documented disaster

Documented episode

The Kakhovka dam was breached on 6 June 2023 during the war, causing catastrophic flooding and major changes to the Dnipro river environment. United Nations reporting documented damage to settlements, disruption of water supply and transport, and hydrological and environmental effects both upstream and downstream. UNEP's rapid assessment used multiple data sources including satellite imagery and remote sensing, while stressing the challenges of assessment in an active conflict zone. [20][21]

What the source supports — and does not prove

The date, flooding and substantial civilian consequences are established. This case does not demonstrate the success of a particular tactical UAV river-defence technique. Rather, it is evidence that a major water obstacle and its adjacent infrastructure can change so rapidly that previously valid terrain and movement information becomes obsolete. It also illustrates the difficulty of independent field verification when access is dangerous or denied.

Lesson learnt

A river should be treated as a changing system. Military intelligence products require time labels, hydrological context and a method for withdrawing or correcting earlier assessments. UAV observations need to be integrated with engineering, water-authority and other independently obtained information. A previously accurate map may become a dangerously misleading basis for decisions.

Southeast Asian relevance and limits

Monsoon river systems, floodplains and deltas can change substantially within the duration of a defensive operation. Southeast Asian water governance, flood patterns, banks, settlements and vessel traffic are regionally specific. The Kakhovka case supports doctrine that anticipates sudden invalidation of previous observations, not a method for locating a river crossing or planning attacks.

National validation question

Can the force recognise and communicate that an earlier river-status report is no longer reliable, and can it replace or qualify that report through a jointly authorised hydrology-and-engineering assessment?

Principal references: [20][21]

A4. Krynky: sustaining a contested river-bank operation

LOCATION / PERIOD Kherson / lower Dnipro | October 2023–2024 • EVIDENCE: AP reporting and attributed testimony

Documented episode

An Associated Press investigation described Ukrainian special-forces preparations and the establishment of a small bridgehead near Krynky on the left bank of the Dnipro in October 2023. The account drew on interviews with participants and reported that earlier planning was disrupted by the Kakhovka disaster. It also described the severe difficulty of sustaining forces in a river environment exposed to enemy fire, drones and difficult weather. The case is instructive because the river was not a neutral line on the map: its condition, access and sustainment requirements shaped the operation. [27]

What the source supports — and does not prove

The reporting establishes that an operation took place and records participants' descriptions of reconnaissance, planning and intense risks. It does not independently verify every individual claim in the source, nor does it justify extrapolating a fixed method of river operation from a small and highly unusual contested bridgehead. Casualty and tactical claims must be handled with particular care.

Lesson learnt

Reconnaissance, command reporting and sustainment are inseparable from riverine planning. Detailed local knowledge may remain incomplete even after extended preparation. In particular, a river operation can lose viability through logistics, weather and the enemy's ability to disrupt access, regardless of whether aerial surveillance remains available.

Southeast Asian relevance and limits

Southeast Asian river defence must allow for dense civilian boat activity, tropical storms, floating vegetation and differing bank conditions. A host force can use the case to challenge optimistic assumptions about observing or supplying a river sector without adopting the specific Ukrainian operation as a model.

National validation question

Can the national command system integrate changing river information, logistics assessments and civilian safety reporting into a single, time-qualified picture without assuming continuous aerial or network access?

Principal references: [27]; regional context [20]

A5. Donetsk and Sumy fronts: adaptation through 2024

LOCATION / PERIOD Eastern and northern Ukraine | 2024; fieldwork Nov 2024–Jan 2025 • EVIDENCE: RUSI field study

Documented episode

RUSI's February 2025 tactical review was informed by fieldwork in several Ukrainian formations on the Donetsk and Sumy fronts during late 2024 and early 2025. It described a highly adaptive contest in which uncrewed systems, electronic warfare, short-term technical advantage, engineering, air defence, logistics and new procedures interacted continuously. This is the appropriate scale at which to examine the operational problem: not one aircraft type, but multiple capabilities changing together. [2]

What the source supports — and does not prove

The findings reflect reputable, direct field-based research, but the authors explicitly characterised the study as field notes rather than a comprehensive academic measurement of every front. The observations should not be turned into universal loss statistics or fixed performance specifications. Units, dates, systems and terrain mattered.

Lesson learnt

The enduring capability may be the organisation's ability to revise training, technical support and doctrine faster than its earlier assumptions become obsolete. Procurement, protected communications and intelligence analysis all require a mechanism for feedback. An unresponsive approval or repair system can render a nominally available UAV fleet operationally ineffective.

Southeast Asian relevance and limits

Southeast Asian forces may face wholly different starting inventories, supply chains, industrial bases and electronic opponents. Ukrainian adaptation is a compelling reason to create a national experimentation and doctrine function; it is not proof that a specific Ukrainian configuration will work under tropical terrain masking or maritime humidity.

National validation question

Is there a formal, rehearsed route from a logged equipment or reporting failure to investigation, nationally authorised SOP amendment, instructor update and repeat validation?

Principal references: [2]

A6. Kherson and other frontline communities: camera precision is not civilian protection

LOCATION / PERIOD Frontline Ukraine, including Kherson | 24 Feb 2022–30 Apr 2025; report Jul 2025 • EVIDENCE: UN verified human-rights evidence

Documented episode

The United Nations Human Rights Monitoring Mission in Ukraine issued a July 2025 assessment documenting 3,030 verified civilian casualties from short-range drones during the period 24 February 2022–30 April 2025. Its work included site visits, interviews and review/geolocation of more than 100 publicly posted drone videos in Kherson region. The report documented the serious humanitarian impact of remotely operated short-range strike systems, including incidents affecting civilian movement and services. The vast majority of verified casualties described in the report occurred in Ukrainian government-controlled territory and were attributed to Russian attacks. [17]

What the source supports — and does not prove

This is a verified harm dataset with described methodology. It is not an estimate of all UAV use, total drone strikes or the comparative accuracy of every side's platforms. It does, however, establish that camera-equipped aircraft and the ability to select a person or vehicle visually do not guarantee compliance with legal obligations or protection of civilians.

Lesson learnt

Armed UAS require distinct command, legal and evidence standards. A recognisable vehicle is not automatically a lawful target. Real-time imagery may be highly detailed yet lack context, identity, time continuity or certainty about civilian presence. Commanders and operators remain accountable and all feasible precautions must be maintained. [12][17]

Southeast Asian relevance and limits

Shared bridges, ferries, plantations, inland waterways and settlements make the distinction between a military objective and civilian activity particularly important for Southeast Asian forces. National doctrine must include a clear and respected authority to suspend, decline or correct actions when information is insufficient. Technical sophistication does not replace human responsibility.

National validation question

Can the national institution demonstrate a separate legal and operational assurance system for armed UAS that treats ambiguous identification and civilian protection as central to readiness, not an appendix to pilot training?

Principal references: [17][28]

A7. JATEC: operational experience translated into an institution

LOCATION / PERIOD Bydgoszcz, Poland; NATO–Ukraine | 17 February 2025 onward • EVIDENCE: official NATO record

Documented episode

NATO and Ukraine formally inaugurated their Joint Analysis, Training and Education Centre in Bydgoszcz on 17 February 2025. NATO describes it as a jointly staffed organisation to analyse lessons from the war, feed them into training and institutional change, improve interoperability and support experimentation. In 2026 NATO publicly reported progress in applying Ukrainian operational insights to training and capability development. [25][26]

What the source supports — and does not prove

This is a documented example of a formal lessons and training institution. It does not establish that a similar structure must be copied by Southeast Asian states or that NATO has endorsed an ADG proposal. The institution's mandates, governance, alliances and funding arrangements are specific to NATO and Ukraine.

Lesson learnt

The important transferable feature is the cycle of structured evidence capture, independent analysis, training and subsequent reassessment. Institutional arrangements make it possible to keep doctrine current and to distinguish recurring failures from exceptional anecdotes.

Southeast Asian relevance and limits

A Southeast Asian sponsor could establish a smaller, nationally governed counterpart function that receives Ukrainian advice but retains sovereignty over curricula, information control, equipment adoption and doctrine approval.

National validation question

Does the national force have an authorised lessons owner, an evidence register, a formal change process, and a means to measure whether lessons have altered training outcomes?

Principal references: [25][26]

ANNEX B | ILLUSTRATIVE SOUTHEAST ASIAN FIELD EXERCISES

These exercises are fictional and are not claimed to be accounts of past Southeast Asian combat. They are bounded, unclassified training concepts to test information integrity, interoperability, environmental fitness and organisational responses when UAS are partially unavailable. Any military implementation must be planned and authorised by the competent national force, with aviation, safety, legal and spectrum controls.

B1. Monsoon-affected mountain corridor

Scenario. A unit must provide a time-qualified route and bridge-condition assessment along a rain-affected mountain road used by civilian traffic.

Exercise conditions. Low cloud; a delayed image; a communications outage; conflicting information from engineers.

Evidence to collect. Completeness and candour of reporting, independent corroboration, acknowledgement time and correct treatment of unseen sectors.

Failure to avoid. Treating one brief observation as continuous clearance or relying on a frozen image as a current picture.

B2. River floodplain with ferries and fishing vessels

Scenario. A joint cell provides river-condition reporting during rising water and intermittent heavy rain.

Exercise conditions. Changing sandbar; civilian boats; suspension of flight by weather; changed bank condition.

Evidence to collect. Hydrology interface, observation timestamps, confidence grading, safe dissemination and withdrawal of stale reports.

Failure to avoid. Assuming a river report remains valid after marked change or conflating civilian traffic with military status.

B3. Dispersed island support network

Scenario. Several geographically separated sites collect infrastructure and maritime condition observations for a joint headquarters.

Exercise conditions. One battery shortage, one delayed resupply, data-bandwidth limitation and a maintenance fault.

Evidence to collect. Ability to distinguish current from historical products, serviceability accounting and prioritised reporting.

Failure to avoid. Reporting full readiness because each site possesses an aircraft even when end-to-end information service has failed.

B4. Dense peri-urban corridor

Scenario. An intelligence cell monitors road condition and emergency-access status in an urbanised environment.

Exercise conditions. Crowded radio environment, buildings occluding observation, civil emergency response and incomplete metadata.

Evidence to collect. Safe task approval; classification of uncertain imagery; reporting corrections; civil coordination.

Failure to avoid. Passing an unqualified sensor label as verified identity or failing to correct a misleading report.

B5. Joint EW and communications assurance tabletop

Scenario. A headquarters must function during simulated connectivity and GNSS uncertainty with multiple friendly electronic systems.

Exercise conditions. Authorized exercise control injects representing intermittent status, misalignment of timestamps and incompatible reporting paths.

Evidence to collect. Accurate failure attribution, escalation, handover, audit trail and avoidance of overclaiming EW resilience.

Failure to avoid. Conducting unauthorised interference tests, hiding self-generated interference or declaring immunity based on limited trials.

ANNEX C | EVIDENCE, UNCERTAINTY AND TRANSFER MATRIX

Issue	Public evidence from Ukraine	Southeast Asian deduction	Required validation
Persistent observation	UAS can significantly improve local awareness, but adversaries adapt.	Can be useful for corridors, rivers and coastlines, with incomplete coverage.	Test actual information quality by terrain, weather and duration.
EW resilience	RF and navigation dependencies are contested; no solution is permanently dominant.	Complex relief and local spectrum use add to operational uncertainty.	Document degraded-mode performance and friendly-system interactions.
Sensor identification	Imagery supports observation but does not automatically resolve identity or intent.	Canopy, haze, river traffic and mixed settlements may elevate ambiguity.	Use blinded analyst trials and preserve uncertain classifications.
River conditions	Ukraine provides limited directly transferable evidence about tropical flood rivers.	Flood cycles and civilian water use can change conditions rapidly.	Joint exercises with engineers and hydrological authorities.
Narrow corridors	Persistent observation can influence movement decisions; routes remain subject to physical constraints.	Bridges, causeways and mountain roads may create information bottlenecks.	Compare aerial findings with engineer and ground reports.
Armed UAS	Weaponised systems have significant effects and substantial legal and technical constraints.	Dense civilian movement and unreliable data may complicate assurance.	Separate authorised, independently reviewed safety/legal acceptance.
Sustainment	Large-scale UAS effectiveness requires workforce, repair and adaptation.	Humidity, corrosion, island logistics and power supply may dominate availability.	Record mission serviceability across repeated and dispersed use.

Interpretation rule: evidence may be sufficient to justify an exercise without being sufficient to justify procurement, operational adoption or a readiness declaration. An absence of public evidence is not proof of impossibility; it is a limit on what a serious independent report may claim. Negative trial findings should be retained with the same care as positive findings.

ANNEX D | NATIONAL SOP DEVELOPMENT AND REVIEW CHECKLIST

D1. Institutional authority

Has a national sponsor designated the lead service, joint author, document owner, approving authority, annual review point and security classification?

D2. End-to-end information standard

Do approved forms state capture time, source, uncertainty, coverage gaps, human review status, report distribution and correction procedure?

D3. Communications assurance

Are aircraft control, sensor transmission and command reporting independently assessed? Are loss/degradation events recorded without inventing the cause?

D4. Environment and seasonality

Are evaluations representative of major terrain and weather conditions? Are monsoon and flood data available to exercise observers?

D5. Personnel and sustainment

Are operators, analysts, maintenance staff, commanders and legal advisers included in collective assessment? Is serviceability tracked during repeated use?

D6. Civilian protection and armed systems

Are lawful authorities and precautionary responsibilities separately documented? Is there an effective process for withholding authorisation in ambiguity?

D7. Version control and revalidation

Can an incident or a verified foreign lesson trigger a documented amendment and repeat evaluation? Are superseded SOPs withdrawn?

D8. National ownership

Are intellectual property, information control, test results, training curricula and final approvals retained by the host state?

ANNEX E | UKRAINIAN PRACTITIONER LESSONS-CAPTURE PROTOCOL

The programme should use a structured and ethically conducted interview method with interpreters and subject-matter verification when required. Practitioners should be free to refuse protected or sensitive operational details. The objective is a useful lesson, not the elicitation of classified procedures. Each record should identify the source's experience level, topic and context while providing appropriate privacy protection.

Context

What was the time period, general terrain, weather, mission function and organisational arrangement? What is the source of the account?

Assumed capability

Which peacetime assumption about aircraft, information, communications, personnel or logistics proved unreliable?

Observed friction

Was the difficulty caused by weather, terrain, friendly systems, an opponent, sustainment, command process or uncertain attribution?

Evidence

Which aspects were directly observed? Which come from post-event analysis, others' testimony, technical logs or inference?

Adaptation

Which institutional practice changed in response? Did the change endure or become ineffective as the environment changed?

Transfer limits

What parts of the experience depend on Ukraine's geography, force structure, equipment, opponent or conflict intensity?

National proposition

What hypothesis could a Southeast Asian defence force test safely and independently within its own environment?

Control and review

Who has verified the translation and context? What information may be retained, shared, taught or published?

Capture template: source identification or anonymised code; date of interview; documented episode; direct observations; corroborating references; uncertainty; institutional lesson; proposed Southeast Asian analogue; recommended national trial; document-control caveats; reviewer; and revision date. A formal register can use the headings as fields rather than treating each interview as a self-validating story.

ANNEX F | REFERENCES AND FURTHER READING

[1] Molloy, Oleksandra. Drones in Modern Warfare (2024–2026): Lessons Learnt from the War in Ukraine. Australian Army Research Centre, 2026. https://doi.org/10.61451/2675166

[2] Watling, Jack, and Nick Reynolds. Tactical Developments During the Third Year of the Russo–Ukrainian War. RUSI, 14 February 2025. https://www.rusi.org/explore-our-research/publications/special-resources/tactical-developments-during-third-year-russo-ukrainian-war

[3] International Institute for Strategic Studies. The Uninhabited War in Ukraine. 2026. https://www.iiss.org/publications/strategic-dossiers/2026/uavs-isr-deterrence-and-war/the-uninhabited-war-in-ukraine

[4] Slusher, Matthew. Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience. CSIS, 2 May 2025. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience

[5] Watling, Jack. Emergent Approaches to Combined Arms Manoeuvre in Ukraine. RUSI, 2025. https://www.rusi.org/explore-our-research/publications/insights-papers/emergent-approaches-combined-arms-manoeuvre-ukraine

[6] Mekong River Commission. Hydrometeorological Monitoring. https://www.mrcmekong.org/hydrometeorological-monitoring/

[7] World Meteorological Organization. State of the Climate in Asia 2025. Published 17 June 2026. https://wmo.int/resources/publication-series/state-of-climate-asia/state-of-climate-asia-2025

[8] International Telecommunication Union. ITU-R P.530-19: Propagation Data and Prediction Methods Required for the Design of Terrestrial Line-of-Sight Systems. 2025. https://www.itu.int/rec/R-REC-P.530/

[9] International Telecommunication Union. ITU-R P.837-8: Characteristics of Precipitation for Propagation Modelling. 2025. https://www.itu.int/rec/r-rec-p.837/en

[10] European Union Aviation Safety Agency. EASA Updates Safety Information Bulletin on GNSS Interference. 3 July 2026. https://www.easa.europa.eu/en/newsroom-and-events/news/easa-updates-safety-information-bulletin-gnss-interference

[11] Markopoulou, Mersini, and Federico Mantellassi. Electronic Warfare and Innovations in Uncrewed Aerial Systems. UNIDIR, 12 October 2026. https://unidir.org/publication/electronic-warfare-and-innovations-in-uncrewed-aerial-systems-arms-control-and-disarmament-implications/

[12] International Committee of the Red Cross. Frequently Asked Questions: International Humanitarian Law and the Use of Drones in Armed Conflict. https://www.icrc.org/en/article/faq-international-humanitarian-law-drones-armed-conflict

[13] International Committee of the Red Cross. Frequently Asked Questions: Autonomous Weapon Systems. 2026. https://www.icrc.org/en/article/faq-autonomous-weapon-systems

[14] International Committee of the Red Cross. Autonomous Weapon Systems and International Humanitarian Law: Selected Issues. 2026. https://www.icrc.org/en/article/autonomous-weapon-systems-and-international-humanitarian-law-selected-issues

[15] International Civil Aviation Organization. Annex 6, Operation of Aircraft, Part IV: Remotely Piloted Aircraft Systems. https://store.icao.int/en/annex-6-operation-of-aircraft-part-iv-remotely-piloted-aircraft-systems

[16] United Nations Department of Operational Support. Rules and Regulations for Unmanned Aircraft Systems. https://operationalsupport.un.org/en/rules-and-regulations-unmanned-aircraft-systems

[17] United Nations Human Rights Monitoring Mission in Ukraine. Deadly Drones: Civilians at Risk from Short-Range Drones in Frontline Areas of Ukraine, 24 February 2022–30 April 2025. 17 July 2025. https://ukraine.un.org/en/298136-deadly-drones-civilians-risk-short-range-drones-frontline-areas-ukraine-24-february-2022-%E2%80%94

[18] Watling, Jack, et al. Preliminary Lessons from Ukraine's Offensive Operations, 2022–23. RUSI, 2024. https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-ukraines-offensive-operations-2022-23

[19] Watling, Jack, et al. Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive. RUSI, 2023. https://www.rusi.org/explore-our-research/publications/special-resources/stormbreak-fighting-through-russian-defences-ukraines-2023-offensive

[20] United Nations Environment Programme. Rapid Environmental Assessment of Kakhovka Dam Breach Ukraine, 2023. 26 October 2023. https://ukraine.un.org/en/250669-rapid-environmental-assessment-kakhovka-dam-breach-ukraine-2023

[21] United Nations in Ukraine. Kakhovka Dam Destruction, One Year On. 6 June 2024. https://ukraine.un.org/en/270890-kakhovka-dam-destruction-one-year

[22] Harding, Luke. The Drone Operators Who Halted Russian Convoy Headed for Kyiv. The Guardian, 28 March 2022. Commander-attributed account. https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv

[23] Rajaratnam School of International Studies. The Russia–Ukraine War: Lessons for Southeast Asia. 2023. https://rsis.edu.sg/rsis-publication/idss/ip23008-the-russia-ukraine-war-lessons-for-southeast-asia/

[24] Reuters. How Drone Combat in Ukraine Is Changing the Face of Warfare. 26 March 2024. https://www.reuters.com/world/europe/how-drone-combat-ukraine-is-changing-face-warfare-2024-03-26/

[25] NATO Allied Command Transformation. NATO and Ukraine Open the Joint Analysis Training and Education Centre. 17 February 2025. https://www.act.nato.int/article/nato-ukraine-open-jatec/

[26] NATO Allied Command Transformation. One Year Later: Advancing NATO's and Ukraine's Transformation. 17 February 2026. https://www.act.nato.int/article/jatec-one-year/

[27] Associated Press. How Ukrainian Special Forces Secured a Critical Dnipro River Crossing in Southern Ukraine. 2023. https://apnews.com/article/5904895c89bf6883dcf8954868295598

[28] United Nations in Ukraine. 2025 Deadliest Year for Civilians in Ukraine since 2022, UN Human Rights Monitors Find. 12 January 2026. https://ukraine.un.org/en/308241-2025-deadliest-year-civilians-ukraine-2022-un-human-rights-monitors-find

Analytical conventions and limitations

References support the broad propositions described in the chapters and source-qualified annexes. They are not a substitute for classified national operating data, technical test reports, evidence from specific Ukrainian formations or independent verification of every reported incident. Where only participant testimony is available, the text explicitly says so. Analytical transfer to Southeast Asia is identified as inference pending host-nation testing.

In this report, UAS means the aircraft and the organisational, technical and human system necessary to operate it. UAV is the aircraft alone. EW is electronic warfare; GNSS is global navigation satellite system; ISR is intelligence, surveillance and reconnaissance; SOP is standard operating procedure. "Direct-attack UAS" describes an armed system category, not an operational instruction. Design and imagery are illustrative unless a source is named.