epik EUROPEAN POLICY INSTITUTE IN KYIV

Opening Ukraine's skies

Design principles for civil-military airspace coordination in a security environment that can no longer be divided cleanly into peace and war.

 Mark Opgenorth

24 April 2026

Jose Luis Stephens, Shutterstock

EXECUTIVE SUMMARY

When diplomacy enables a full reopening of civilian airspace over Ukraine, it will be governed differently from how it was before 2014. Russian revisionism and the drone revolution mean that civilian air traffic will face a persistent, variable threat even after sustained aerial bombardment has ended.

However, the challenge will not be Ukraine's alone: it will be continental. Drone incursions and interference with navigation systems forced airport closures across Europe in late 2025, while the March 2026 Middle East crisis has exposed the same structural gap. There is no institutional channel for connecting military threat awareness to civilian operational decisions. The gap is a Cold War inheritance: separate institutions for peace and war but nothing built for conditions between the two. Without a characterised threat assessment or graduated response options, civilian controllers face a binary choice: normal operations or shutdown.

"Hybrid threats" in the EU sense are campaigns that rather than attack any single sector in isolation, deliberately target vulnerabilities at the interfaces between institutions and levels of governance. In airspace, that interface is the seam between military threat awareness and civilian operational control – the space where today no institution is equipped to act.

This paper sets out design principles for civil-military airspace coordination in a security environment that can no longer be divided cleanly into peace and war. It proposes a staged programme of capability development – from coordination infrastructure through unmanned corridor operations to crewed cargo – that serves defence today and builds towards civilian air connectivity as conditions evolve, positioning Ukraine as a co-designer of the next generation of civil-military airspace governance.

FROM DEADLOCK TO DESIGN

Ukrainian airspace has been closed to civilian aviation since 24 February 2022. No Ukrainian airport has handled a commercial flight in over four years. Three interconnected barriers prevent reopening: (a) a security barrier, as Russian missiles and drones can reach any point in Ukrainian territory and air defence cannot eliminate the risk; (b) an insurance barrier, as no insurer will underwrite risk that cannot be quantified; and (c) a regulatory barrier, as the European Union Aviation Safety Agency (EASA) cannot reassess its conflict zone bulletin without evidence of mitigation, but such evidence cannot be generated without infrastructure and procedures that do not yet exist. These barriers are mutually reinforcing and no single actor can break the cycle alone.

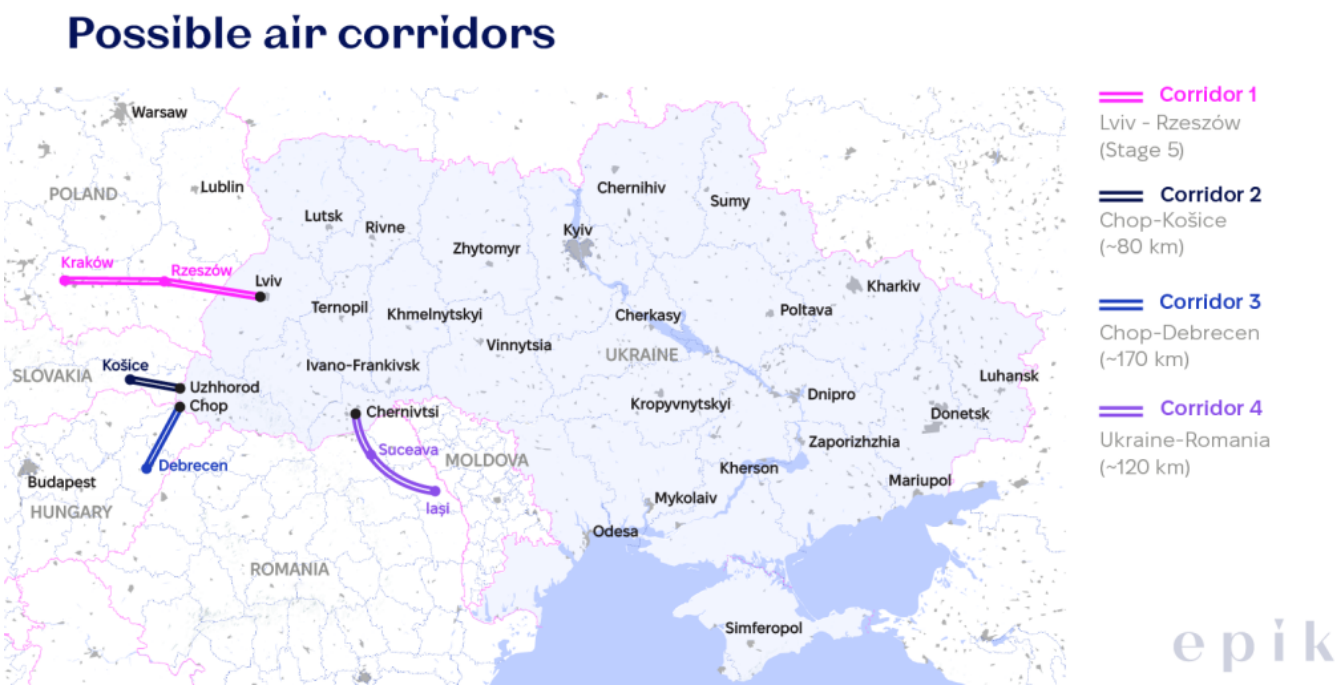
A roadmap for reopening Ukrainian airspace was presented at an aviation industry event in Warsaw in October 2024, backed by significant diplomatic and commercial support. Expectations ran high. One senior industry figure publicly suggested that flights from Lviv or Boryspil could resume by early 2025 and several airlines were prepared to recommence operations. The initiative attempted to break the deadlock through political momentum. When the proposal entered the interagency process, however, the authorities responsible for airspace security and safety kept the existing closure in place.

The failure of the initiative reflects not a lack of political will, but a problem of campaign design. It sought a dispensation – political approval to resume flights – from officials who bear civil and criminal liability for aviation safety. In the absence of a framework for any state between full closure and full opening, the campaign was asking them to accept a risk they had no tools to manage. They could only say no.

The nature of the risk reinforces this dynamic. Conventional aviation risks such as engine failure or wind shear follow probability distributions that insurers can price. Conflict risk is fundamentally different. It is generated by adversaries who observe defences and deliberately circumvent them. The risk changes shape in response to the measures taken against it, which means that conventional insurance models cannot price it[1]. Managing adversarial risk requires a different kind of data that is continuous, location-specific and capable of characterising an adversary's evolving capability and intent. No single institution possesses such data. The problem is architectural.

A different question yields a different dynamic. Not "grant us permission to fly" but "what must be built so that Ukraine is ready to open its airspace progressively, as conditions evolve?" The first seeks a dispensation; the second builds a capability. In March 2026, Ukraine's Ministry for Communities and Territories Development established a cross-ministerial working group "on the preparation for restoring" airport operations, bringing together civil aviation, military, security and infrastructure authorities alongside the directors of Boryspil and Lviv airports.

The working group's composition, which spans the full range of civil and military authorities responsible for airspace management, is exactly right. The question is how to structure its work so that it produces concrete, cumulative results across short-, medium- and long-term horizons, rather than rehearse the appeal that went nowhere in 2024. This paper offers a framework for that effort. It does not lobby for a decision; it seeks to build a capability. Nothing in it requires a decision to reopen airspace. Everything in it strengthens national defence today and builds civilian air connectivity for tomorrow.



SHUTDOWN BY DEFAULT

The architectural problem is not Ukraine's alone; it is built into how airspace is governed everywhere. Civilian aviation authorities manage air traffic, enforce safety standards and bear regulatory accountability. Military authorities maintain threat awareness, control air defence and bear the consequences when threats are not countered. Each possesses half of what is needed to manage airspace under contested conditions and no institutional channel connects the two. The military picture – what is in the sky, where it came from and what it is likely to do – exists on one side of a wall. The civilian decision-making authority – whether to permit, restrict or halt operations – exists on the other. When a threat appears, the controller on the civilian side receives no characterisation of it. Without such a characterisation, the only defensible response is shutdown.

European airspace has already faced the same condition. In the final months of 2025, drone incursions forced repeated airport closures across Europe. Copenhagen Airport alone suspended operations for nearly four hours after multiple drones entered controlled airspace – a single incident that affected 20,000 passengers and cost an estimated €6.5–15 million. Munich, Brussels and Vilnius followed. At Vilnius, balloons launched from Belarus triggered 15 closures between October and December, disrupting over 350 flights. In parallel, GPS jamming and spoofing attributed to Russian electronic warfare has become routine. Reported disruptions have increased by more than 200 per cent since 2021.

The scale of disruption has provoked a formal institutional response. In June 2025, ministers from 13 EU member states signed a joint letter demanding coordinated action. In February 2026, EASA and Eurocontrol published a joint action plan for operating under satellite navigation interference. It is the first of its kind, built on the explicit assumption that interference "will persist for the foreseeable future". Nonetheless, the same pattern recurred at every affected airport. There were no intermediate protocol, no graduated options and no military threat characterisation to inform a calibrated civilian response.

What these closures share is not just the absence of a protocol, but a deeper structural condition. NATO's civil-military cooperation doctrine recognises that the civilian environment – its infrastructure, services and dual-use systems – is not separate from military operational considerations but already within them. In doctrinal terms, this is the "civilian battlespace". This concept is useful insofar as it acknowledges that airspace is a single operational environment regardless of whether the actors within it are civilian or military, but it sees this only from the military side, mapping civilian terrain as part of its operational picture. It does not give the civilian side a corresponding framework for receiving and acting on military threat assessments. Nor does it specify the coordination architecture, graduated response protocols or filtered data pipelines that would allow both sides to govern shared airspace while retaining their distinct authorities. The repeated airport closures across Europe are not failures of peacetime aviation management that spilled into a military domain. They are failures to govern airspace as the shared operational environment it has always been – failures that neither the military nor the civilian framework, as currently designed, can resolve alone. This paper attempts to specify an architecture that bridges them.

It is important, however, to distinguish the military capability problem from this institutional coordination problem and then bring them back together. Much of the European discussion about the drone threat – and much of the investment flowing from initiatives like the EU's Drone Defence Initiative and the European Sky Shield – focuses on the military response – the need for cost-effective counter-drone capabilities, interceptor systems that can engage cheap drones without wasting expensive missiles and layered air defence that does not depend on fighters and high-end surface-to-air systems designed for a different class of threat. These are real and urgent gaps. Even if they are fully bridged, however, and even if every European state fields effective, affordable counter-drone systems, the institutional coordination problem remains. A military with robust counter-drone capabilities still cannot, under current arrangements, deliver a characterised threat assessment to the civilian controller who must decide whether to close, restrict or continue operations. Resolving the military capability problem without resolving the coordination problem means that airports will still close every time a drone appears – not because the military cannot manage the threat, but because the civilian controller has no

authorised basis for any response other than shutdown. This paper addresses that coordination problem.

The March 2026 Middle East crisis illustrates the point in an adjacent region. When Iranian missiles and drones struck across the Gulf, every affected state improvised its own airspace response. Iran, Iraq, Kuwait and Syria closed entirely. The United Arab Emirates (UAE) oscillated between full closure, partial reopening through a single western corridor and brief precautionary shutdowns. Jordan instituted daytime-only operations and nightly closures. Saudi Arabia kept routes open on contingency routings while restricting areas near active military operations. EASA carved a narrow altitude-restricted corridor through otherwise prohibited Omani and Saudi airspace. These were not pre-designed operating states – they were improvisations under fire, conducted without a shared regional framework because no institution in the Gulf performs the coordination function that Eurocontrol performs, however incompletely, in Europe. As the crisis continued, Gulf states sought Ukrainian counter-drone expertise in a recognition of the world-leading capabilities Ukraine has developed under the pressure of war. Even the arrival of those capabilities did not resolve the airspace governance problem. The military capability to engage the threat can be transferred from those who have it to those who need it; what is missing everywhere is the institutional architecture to translate that capability into graduated, coordinated airspace management.

The European disruptions, the Gulf crisis and the Ukrainian closure are not separate problems. They are the same structural gap at different points along a spectrum: Ukraine pressing from war towards peace; Europe being drawn from peace towards threat; and the Gulf states thrust overnight from peacetime into missile attack with no institutional preparation for the transition. Russia's sustained campaign of destabilisation across Europe and Iran's persistent destabilisation of Middle East security – two adversaries pursuing varied means towards the same end of undermining the rules-based order – make clear that this is not a temporary condition but a structural feature of the security environment.

In EU terms, this is a hybrid threat environment – deliberate adversarial pressure applied across domains and at the interfaces between civilian and military responsibility, where no single authority has clear tools to respond. The airspace governance gap addressed in this paper is one such interface.

The gap is a Cold War inheritance built in two layers. The 1944 Chicago Convention establishes "complete and exclusive sovereignty" of each state over its overlying airspace, so every cross-border coordination arrangement must be negotiated state by state and no EU institution can impose a unified framework. Within each state, civil and military responsibilities were then divided between separate institutions designed for different conditions. The EU's Flexible Use of Airspace, formalised in 2005,

manages the peacetime problem. The competition for space between military exercises and civilian routes is resolved through advance scheduling. There is no mechanism for real-time military threat characterisation to reach civilian controllers. NATO Air Policing manages the wartime side through continuous surveillance and interceptors on alert, but this military situational awareness runs parallel to civilian air traffic management rather than feeding into it. Even if a NATO Combined Air Operations Centre knows precisely what an unidentified object near an airport is, there is no standing pathway for delivering that assessment to the civilian controller deciding whether to close.

European institutions have acknowledged the need for change. Eurocontrol's Civil-Military Cooperation Division has prioritised adaptation to the changed security environment. The Commission's Defence Readiness Roadmap announced a European Drone Defence Initiative intended to be fully interoperable for civil-military and dual-use purposes. The EU's Counter-Drone Action Plan of February 2026 calls for a shared situational awareness system accessible to civil aviation, law enforcement and military authorities. At the national level, Germany inaugurated the Joint Drone Defence Centre in Berlin in December 2025, staffed jointly by the Bundeswehr, the Federal Police and the Federal Criminal Police Office. Belgium approved a National Airspace Security Centre at Beauvechain air base, integrating the Air Component, the Federal Police, Customs and the civil aviation authority into a single counter-drone command hub. Each of these responses crosses the peacetime institutional boundary between civilian and military airspace responsibility. Together, they amount to an explicit acknowledgement that the peacetime architecture is no longer adequate and they all point in the same destination towards fused civil-military situational awareness for airspace management.

One country has resolved the civil-military problem by eliminating the boundary altogether. Israel's Air Force has overarching responsibility for national airspace. Civilian operations are managed within the military operational picture. This is the operational expression of MABAM (ha-ma'arakha she-bein ha-milkhamot, the "campaign between wars") – a doctrine that rejects the peace/war binary in favour of continuous military operations across every domain. The model demonstrates that civil-military fusion is operationally achievable. The results are manifest: Ben Gurion Airport has operated through multiple escalation cycles using graduated measures – adjusted approaches, tactical pauses and rapid resumption – rather than the blanket closures that European airports default to under far lesser threats.

The Israeli model works because of two conditions that no European state shares: a society organised around permanent security mobilisation and a single small airspace against the sea with little need for cross-border coordination. For Ukraine, the operational logic might seem to fit – a country at war, with airspace closed and military authority already paramount – but Ukraine's strategic direction points

towards Europe and the European framework requires both things Israel's model dispenses with – independent civilian safety regulation and an airspace governance structure designed to work across borders. Ukraine's commitment to adopting the EU aviation acquis – with its independent regulator, certification framework recognised across 44 states and cross-border integration architecture – provides the foundations for what it needs to build.

DESIGN PRINCIPLES

An architecture is required in which military threat awareness continuously informs civilian operational decisions across conditions that are neither fully peace nor fully war, and through the transitions between them. Because airspace is a single operational environment regardless of whether the actors within it are civilian or military, this architecture must function across the full spectrum of threat. In effect, it must give civilian authorities an operational capacity in the hybrid seam between peace and war, civilian safety and military defence.

Two core requirements define this architecture:

- **Shared situational awareness, not shared command.** A filtered data pipeline from military situational awareness to civilian operational displays in which military authorities retain their classified picture and engagement authority and civilian authorities retain their regulatory independence. What changes is that civilian decisions are informed by military assessments rather than made in ignorance of them. The filtering mechanism – what data is shared at what classification level, in what format and with what latency – will be the central design challenge. The counterintelligence dimension of this filtering must be addressed in the architecture's design, not deferred as an afterthought.
- **Graduated response, not binary shutdown.** The architecture must support multiple operating states between "normal" and "closed". Defined threat levels, specified operational modifications at each level, clear escalation and de-escalation triggers and pre-delegated decision-making authority would enable civilian operations to continue under variable threat levels by adapting to conditions rather than ceasing entirely. Jordan's day/night regime, the EASA corridor exception in southern Saudi Arabian and Omani airspace, and the UAE's controlled corridor system all demonstrate that a graduated response is operationally necessary. The only question is whether such a response is designed in advance or improvised under fire.

Four enabling conditions follow from these core requirements:

- **Layered communications resilience.** Civil-military airspace coordination depends on communications that function under adversarial conditions – not just in peacetime, but precisely when GPS is jammed, signals are spoofed and standard systems are degraded or denied. NATO joint doctrine captures this in the PACE framework (Primary, Alternate, Contingency, Emergency). The layers run from standard civilian communications through hardened alternatives and tactical mesh networks to procedural control as a last resort. The critical gap is the contingency layer. It does not currently exist in any European civilian airspace system and no technology has been designated for it. However, it is the layer that matters most as it must function precisely when the layers above it have been denied. Military operations in Ukraine have demonstrated that mobile ad hoc network (MANET) tactical radios can sustain communications under exactly these conditions and the US Air Force already uses MANET for expeditionary airfield operations worldwide. The gap is not technological: it is institutional.
- **Persistent sensor infrastructure.** Low-altitude threat detection requires permanent multi-sensor networks, not radar systems designed for commercial aircraft at altitude. Open sensor-fusion standards are being adopted by NATO, making multi-vendor integration technically viable. The same sensor infrastructure that serves airspace security serves the surveillance requirements for commercial drone traffic management under U-space, the EU's regulatory framework for managing low-altitude unmanned traffic. This is a capability that has been regulated but not yet delivered. Defence needs alone will not sustain the required sensor density; only a functioning civilian drone market will.
- **Cross-border integration by design.** Any corridor involving Ukrainian and neighbouring airspace must be designed for cross-border operation, with interoperable systems, shared data formats and pre-agreed coordination procedures.
- **EU regulatory compatibility from the outset.** Ukraine's EU accession path requires alignment with the Single European Sky but the Single European Sky does not prescribe a single institutional model for civil-military coordination. Integration must be organised transparently, formalised in documented arrangements and subject to independent safety oversight. An architecture designed with these principles satisfies accession requirements while producing a working model that can inform broader European reform.

THE INSTITUTIONAL PATH

If the Israeli model is politically impossible and the status quo is operationally inadequate: which institutional path can deliver the upgrade? Three immovable constraints narrow the field: the Chicago Convention makes airspace sovereignty national, the EU acquis requires civilian regulatory independence and the threat environment is transnational.

Eurocontrol is the only institution that respects all three constraints. It is a civil-military intergovernmental organisation with 41 member states that span NATO, the EU and partner countries, Ukraine among them. It already operates tools that merge civil and military data sources into a correlated air situation display deployed at air defence units across NATO states, and provides real-time airspace status and cross-border coordination. Its Civil-Military Cooperation Division has reoriented its strategy to accommodate security and defence needs, and the European Commission's Counter-Drone Action Plan has identified Eurocontrol's civil-military data-fusion tool as the platform for real-time drone threat detection and identification.

However, Eurocontrol's current toolkit is essential but insufficient. Its civil-military data-fusion tool merges surveillance and flight plan data and is widely deployed at air defence centres and other military sites, with air traffic control fall-back functions and limited use by the civil side in some states. However, a filtered pipeline from NATO-level or national military situational awareness to civilian operational displays at ordinary air traffic control consoles does not yet exist as a network-wide standing capability. There is currently no Eurocontrol tool that encodes operational responses linked to specific threat characterisations, and no existing pan-European framework defines graduated operating states with pre-delegated decision-making authority for civil aviation operations. The EASA-Eurocontrol action plan on satellite navigation interference assumes that interference will persist and organises many of its measures on multi-year timelines that do not match the tempo at which interference incidents are already occurring. The upgrade required is not merely institutional but conceptual: from scheduling coordination to threat-informed operational coordination.

A NATO-led model would have military credibility but exclude non-NATO EU member states, lack regulatory authority and risk militarising civilian governance. An EU-only model through EASA would have regulatory authority but no military participation. National solutions, such as Germany's Joint Drone Defence Centre or Belgium's National Airspace Security Centre, resolve the problem within borders but not across them. The Gulf crisis demonstrates the cost of having no multilateral coordination framework at all. Recent initiatives, such as the EU's Counter-Drone Action Plan and Eurocontrol's evolving civil–military cooperation strategy, point in this direction by emphasising shared situational awareness

and real-time drone threat detection, but they stop short of specifying a threat-based regime of graduated civilian operating states.

What is needed, and what this paper proposes, goes beyond what any of these institutions currently offers in operational form: a design concept that connects military threat characterisation to civilian graduated response through a standing, filtered, real-time data pipeline implemented through the Eurocontrol framework but extending its capabilities from data fusion into operational decision support.

UKRAINE AS CO-DESIGNER

In March 2026, the EU informally opened all six accession clusters for negotiation, including Cluster 4, the Green Agenda and Sustainable Connectivity, which encompasses transport policy and the Single European Sky. No EU member state has yet fielded what the EU's own policy documents describe. This is not a deficit but an opening, however, as Ukraine can build with European institutions rather than retrofit after them.

The partnerships already exist, from Eurocontrol recovery support to air traffic controller refresher training with French and Romanian providers, Swedish cooperation on surveillance and remote towers, and a Leonardo-ENAV donation of five primary radar systems, but these are seed-scale commitments. The reconstruction ecosystem operates at a different order of magnitude involving EU recovery packages, EBRD financing exceeding €9.1 billion and the planned European Flagship Fund. It is the dual-use framing that connects them. Infrastructure that serves both defence and civilian purposes can attract reconstruction grants, defence aid, EU accession investment and private capital. Without this framing, airspace coordination must compete for scarce sector funding; with it, the corridor becomes one component of an investment architecture already being built.

If Ukraine designs its architecture with these requirements, the result will be not mere accession compliance but a reference implementation – a working model of what European states are trying to build but have not yet achieved. The sensor data flows. A drone corridor approved under the EU's risk assessment framework proves the architecture under real conditions in a world first in a conflict-adjacent zone, translating Ukraine's military drone leadership into a regulated civilian framework. The insurance facility evaluates the data. EASA reviews the corridor-specific risk assessment. Controllers train on the fused operational picture. When a political or security window opens – through ceasefire, coalition deployment or evolution of the threat – the corridor is ready to scale from unmanned to crewed operations, not in years but in weeks.

THE PEACE PROCESS WINDOW

The programme would deliver value regardless of how the conflict evolves, but it would be particularly well positioned to capitalise on opportunities that a ceasefire might create. However, the window for shaping those opportunities is narrow. The Paris Declaration of January 2026 established a Coalition of the Willing framework with elements directly relevant to airspace governance, notably monitoring and verification mechanisms, reassurance measures in the air and an air policing mandate. However, the civilian aviation community is not at the table where these elements are being designed.

The cost of this absence is measurable. In Kosovo, the 1999 Kumanovo Agreement assigned the NATO-led peacekeeping force commander control over all airspace with a provision that civilian control would be delegated "as soon as practicable". Because civilian aviation requirements were not built into the original military framework, it took 15 years to reopen upper airspace and 21 years to restore lower airspace routes. The Sinai Multinational Force and Observers offers a contrasting model from 1981. Graduated zone-based provisions and continuous aerial verification created a stable, quantifiable security environment that enabled civilian activity to resume and expand. The difference was design intent – whether civilian requirements were incorporated from the outset or left to be retrofitted after the fact.

The working group's mandate extends naturally into this dimension, ensuring that Ukraine's ceasefire preparations include the civilian aviation architecture. Three provisions would directly enable corridor operations if incorporated into a ceasefire framework. First, airspace deconfliction provisions that define graduated zones with specified security conditions, creating the regulatory preconditions for an EASA corridor-specific assessment rather than a blanket restriction. Second, monitoring data architecture structured from the outset with dual outputs – a classified stream for military and diplomatic consumers, and an appropriately filtered stream formatted for civilian regulators and insurers. Third, air policing mandates drafted to encompass protection of defined civilian corridors – not merely military deterrence – so that the Coalition's air component becomes part of the layered security architecture that enables civilian operations.

None of these require anyone to commit to reopening Ukrainian airspace. They require only that ceasefire provisions are drafted with the civilian aviation dimension in mind. The corridor architecture described in this paper is designed to withstand deliberate disruption – a requirement that does not depend on whether a ceasefire holds. The window for influencing ceasefire design is open now,

however, and once provisions are in place, retrofitting them for civilian purposes will be far harder than incorporating the requirement from the outset.

RECOMMENDATIONS

This paper does not argue for passenger flights under current conditions. It does not seek a dispensation to fly. The programme asks nothing of the security establishment that conflicts with its mandate. It asks it to guide investment in capabilities that strengthen national defence. Passenger operations will remain unacceptable until there is a fundamentally different strategic environment, involving changed Russian capabilities and intent and NATO air-defence guarantees. The architecture required for that future cannot be improvised when conditions change, however, but must be built in advance – and building it serves defence needs today.

The programme below is designed to give the working group a structured path from actions that strengthen national defence through to readiness for civilian air connectivity. Each element generates deliverables that justify the investment on security grounds alone. The first four workstreams are parallel, not sequential. Progress on each reinforces the others.

The programme carries risks that must be managed openly. Graduated architectures can create ambiguity about decision rights under pressure; shared situational awareness, poorly designed, can compromise intelligence sources; and any programme building towards civilian operations in a conflict zone will face accusations of normalising risk. These risks are addressed through clear pre-delegation protocols, rigorous counterintelligence review of the filtering mechanism and transparent communication that this is a capability-building programme, not a fait accompli.

- **Coordination Architecture and Communications Infrastructure.** The first requirement will be a standing facility where military and civilian airspace management personnel work from common data systems with appropriately filtered views of the same operational picture – the institutional expression of shared situational awareness. Ukraine is better positioned to build this than most European states. The Delta situational awareness platform already provides multi-domain operational awareness with layered, permission-based filtering built into its architecture. This is a national capability that European states have yet to replicate and the Working Group provides the institutional foundation. The facility will need a communications backbone built for adversarial conditions – layered from standard systems through hardened alternatives to tactical mesh networks and tested in a corridor in western Ukrainian airspace. Every element would serve defence today: air defence,

drone coordination and critical infrastructure protection. The resilience data it generates is what regulators and insurers will eventually require.

- **Cross-Border Engagement and Corridor Definition.** The corridor concept should not be confined to a single border. Poland is the obvious starting point but a short drone corridor across the Transcarpathian border with Slovakia or Hungary, which is less congested and less militarised, might prove easier as an early proof-of-concept. Romania's eastern border already serves as a gateway for military deliveries and would benefit from the same infrastructure. Pursuing multiple corridors in parallel would create resilience in the diplomatic process itself as a track that stalls in one direction might advance in another. All of this would proceed at the technical level without requiring political decisions about civilian flights.
- **Regulatory Framework and Insurance Architecture.** The corridor would generate something no previous initiative has produced: continuous, location-specific data on the actual threat environment – how often threats appear, how effectively they are countered and how reliably communications and navigation systems perform. Such data would transform the regulatory problem. EASA's conflict zone methodology can evaluate a defined corridor; it cannot evaluate an entire country at war. The same data can address the insurance barrier. Insurers have indicated a willingness to underwrite corridor operations, but only if the risk can be quantified from observed performance rather than estimated from general conditions. Both the regulatory assessment and the insurance facility can be developed while the corridor operates unmanned, converting infrastructure into commercial readiness without requiring crewed flights.
- **Unmanned Corridor Operations.** Just as the corridor reduces the airspace problem from a country to a defined segment, unmanned operations reduce the risk problem from passenger safety to cargo and logistics – a scope that existing EU regulation can already handle. The SORA framework provides a structured methodology for authorising drone operations with risk mitigations tailored to corridor, environment and threat. A cross-border drone corridor operating under SORA approval in a conflict-adjacent zone would be a world first. Ukraine has developed world-leading military drone capabilities – design, manufacture and operations at scale – but the pressure of war has left civilian use cases and safety regulation undeveloped. A SORA-approved corridor would bridge that gap, translating military drone expertise into a regulated civilian framework and opening a path to the commercial drone economy that Ukraine's technical base is well positioned to serve. This is the pivotal demonstration as the architecture from the other workstreams proves itself under real conditions, generating the track record that insurers, regulators and decision makers require before crewed

operations can be contemplated.

- **Crewed Cargo Operations and Scaling.** Each preceding stage narrows one dimension of the problem – geography, then risk category, then regulatory scope. This stage begins to widen them again, progressively, from unmanned to minimally crewed cargo as certification develops, then to conventional crewed freight. The commercial case is immediate. High-value Ukrainian exports currently bear the cost and delay of road transit to European airports, while deliveries to Ukraine, including time-sensitive military goods, face the same bottleneck in reverse. Operations are governed by the graduated response system built into the coordination workstream, scaling-up as threat data and conditions permit – increasing traffic volumes, expanding operators and potentially extending to passenger services. None of this is dependent on predicting the conflict's trajectory.

The working group has the right composition and the right mandate. What it needs is an approach that builds capability, not one that seeks dispensations. That is what this paper offers.

Mark Opgenorth is a co-founder of the Kyiv-based Rapid Capability Group and Director of Polemos Technology UAB, a Vilnius-based mission engineering firm. He has previously served as a staff officer at NATO and as a Canadian foreign service officer.

1

Ellison stated that passenger aircraft such as the Airbus A320 and Boeing 737 would require insurance cover of at least $750 million to resume flights to Ukraine. The figure reflects global airline liability norms but cannot be justified on actuarial grounds without the continuous, corridor-specific threat data that a new civil-military architecture would have to generate. Ibid.