TLP:CLEAR

AIRPORTS COUNCIL INTERNATIONAL

Hybrid Threats and Airport Resilience

ACI EUROPE STRATEGY PAPER

ACI EUROPE Aviation Security Committee



Document Control

Document Details

Document Title	ACI EUROPE Strategy Paper on Hybrid Threats and Airport Resilience
Classification	TLP CLEAR
Version Number	1.0
Status	Active

Author & Owner Details

Author	ACI EUROPE Aviation Security Committee
Owner	ACI EUROPE
Approved For Release By	ACI EUROPE Aviation and Cyber Security Director

Next Review Date

Next Review Date	Undefined

Version History

Version	Date	Comments	Reviewed by
0.1		First Draft	ACI EUROPE
0.2		First review by members	Strategy WG
0.3		Restructure of input	ACI EUROPE
0.4		Second draft	ACI EUROPE
0.5		Additional input included	Strategy WG
0.6		draft for Committee review, version control	ACI EUROPE
0.7	08/10/2026	Final draft for board endorsement	ACI EUROPE
1.0	26/10/2026	Following endorsement by ACI EUROPE's board	ACI EUROPE

Contents

Contents

Contents 3

1. Executive Summary 5

2. Introduction 6

2.1. Defining Critical Infrastructure in the Airport Context 7

2.1.1. Operational Continuity (Business Resilience) 8

2.1.2. Critical Function Continuity (Societal Resilience) 8

2.2 What Needs to Be Protected 9

2.2.1. Core Operational Functions 9

2.2.2. Critical Systems and Technologies 9

2.2.3. External Dependencies 9

2.2.4. Organisational and Decision-Making Capability 9

2.2.5. Public Trust and Information Integrity 10

3. Airports as Strategic Infrastructure within Europe's Critical Infrastructure Ecosystem 10

4. Understanding Hybrid Threats in the Airport Context 11

5. The Evolving Threat Landscape 12

5.1. Drone Activity and Asymmetric Airspace Disruption 13

5.2. Balloons and Low-Tech Cross-Border Disruption 13

5.3. Cyber Threats and Digital Pressure 14

5.4. GNSS Jamming, Spoofing and Navigation-Related Disruption 14

5.5. Physical Sabotage and Off-Airport Vulnerabilities 14

5.6. Human Factors, Insider Threats and Security Culture 14

5.7. Disinformation, Social Media and Perception-Based Disruption 15

5.8. Cascading and Multi-Domain Scenarios 15

6. What Airports Are Doing Today 15

6.1. Different Starting Points and Levels of Maturity 16

6.2. Strengthening Technical and Operational Capabilities 16

6.3. Building Cross-Functional Governance and Situational Awareness 16

6.4. Scenario-Based Exercises and Adaptive Planning 17

6.5. Strengthening Cooperation with Authorities and External Partners 17

6.6. Emerging Practices and Lessons Learned 17

7. Key Challenges and Gaps 18

7.1. No Common Governance Model — and Often No Clear Owner 18

7.2. Business Continuity Is Necessary — but Not Sufficient 18

7.3. Information Provided by State Authorities Remains Inconsistent and Often Insufficient 19

7.4. Existing Frameworks Are Not Sufficiently Aviation-Specific 19

7.5. Funding and Cost-Sharing Remain Unresolved 19

7.6. A Common European Framework Is Still Missing 19

8. Way Forward – 5 Key Principles 19

8.1. Hybrid Threats Against Airports Must Be Recognised as a Strategic Critical Infrastructure Issue 20

8.2. Airport Resilience Must Be Approached as an Integrated, Cross-Functional Capability 20

8.3. State Support and Operationally Useful Intelligence Are Essential 20

8.4. Existing Policy and Regulatory Frameworks Must Better Reflect Airport Realities 21

8.5. Hybrid Resilience Requires Structural Investment and Clearer Cost-Sharing Principles 21

9. Policy Recommendations 21

9.1. Recommendations to EU Institutions 21

9.2. Recommendations to National Governments and Authorities 22

9.3. Recommendations to Airport Operators 22

10. Conclusion 22

1. Executive Summary

European airports are operating in a markedly changed threat environment. Hybrid threats are increasingly affecting operations, security, societal resilience and public trust. They combine elements of cyberattacks, physical sabotage, technological disruption, information manipulation and other asymmetric tactics — often with unclear attribution, cross-cutting consequences and the potential to trigger simultaneous or mutually reinforcing incidents.

For airports, this means that the traditional separation between aviation security, cyber security, operations, business continuity and crisis management is increasingly challenged by a more complex and interconnected risk environment.

As strategic infrastructure within Europe's wider critical infrastructure ecosystem, airports are particularly exposed. They are open, complex and highly integrated systems with critical dependencies on energy, telecommunications, digital networks, navigation systems, supply chains and a wide ecosystem of public and private actors. Disruption in one part of the system can quickly have consequences far beyond the individual airport and affect the wider European aviation network.

European airports are already actively strengthening their resilience. This includes investments in cyber security, counter-drone capabilities, perimeter awareness, crisis management, exercises, redundancies and broader resilience measures. However, these efforts have developed under different national, regulatory and operational frameworks, resulting in a fragmented maturity landscape across the sector.

At the same time, experience across European airports points to several recurring challenges:

- the absence of a common understanding and operationalisation of hybrid threats
- the lack of clear and mature cross-functional governance
- limited and often insufficient information-sharing from public authorities
- frameworks and requirements that do not adequately reflect the specific complexity of aviation
- lack of clarity regarding responsibilities and capability expectations
- lack of adequate funding

ACI EUROPE considers that hybrid threats affecting airports can no longer be treated as a narrow specialist issue. They should be understood as a growing and critical strategic challenge to Europe's wider critical infrastructure ecosystem and as a core resilience issue for the European aviation sector. As such, they are also part of and support the EU's wider strategic autonomy, security and defence preparedness agenda.

ACI EUROPE therefore calls for a more integrated, intelligence-informed and resilience-based approach, supported by:

- closer cooperation between airports and public authorities
- better information-sharing and more operationally useful support
- a clearer aviation-specific anchor in European and national frameworks
- more systemic cooperation, learning and governance across the sector
- greater clarity on responsibilities
- adequate funding

This strategy paper sets out ACI EUROPE's view of the challenge and presents concrete recommendations for EU institutions, Member States, authorities and airport operators.

2. Introduction

Europe's security context has changed dramatically in recent years. Geopolitical tensions, technological developments, increased strategic competition and the more active use of hybrid tactics have created a more complex and less predictable risk environment for critical infrastructure across Europe.

Hybrid threats are characterised by the combination or coordination of pressure across different domains — including cyber, physical sabotage, information operations, technological disruption and interference with essential societal functions. They often operate in the grey zone between peace, crisis and conflict, and are intended to create uncertainty, friction, loss of trust, resource strain and societal disruption.

For airports, this evolution is particularly relevant.

Airports are open, complex and highly interconnected environments where a wide range of public and private actors operate side by side. At the same time, they function as key transport and mobility hubs and depend on a broad range of external infrastructures and technological systems. This combination makes airports attractive targets for both direct and indirect forms of interference, including:

- drone activity affecting airspace and operations
- cyberattacks targeting airports and their supply chains
- GNSS jamming and spoofing
- sabotage or vulnerabilities in external and downstream infrastructure
- misinformation and influence activity
- activism and incidents with high public and media visibility
- low-tech but strategically disruptive incidents involving airborne objects or balloons in sensitive airspace environments

Experience from the Baltic states in particular underlines this development. Incidents involving balloons and so-called "weather balloons" drifting across borders — including from Belarus — have illustrated how even simple and low-tech means can generate uncertainty, operational strain and the need for coordinated response in sensitive airspace environments.

These developments show that airports are increasingly operating in a threat environment in which disruption does not necessarily follow traditional patterns or fit neatly into established categories. It is the combination, simultaneity and ambiguity of incidents — rather than their individual technical nature — that increasingly tests resilience.

It is equally clear that many existing operational, organisational policy and regulatory approaches were designed for a different threat environment. Many of the tools and governance logics that have historically supported airport security and preparedness remain relevant, but they are no longer sufficient on their own to address a more complex and cross-domain hybrid pressure environment.

Against this backdrop, a more mature, integrated and common European approach is needed to how airports understand, organise and strengthen their resilience against hybrid threats.

2.1. Defining Critical Infrastructure in the Airport Context

The concept of "critical infrastructure" is widely used across European policy frameworks, but its meaning remains both context-dependent and inconsistently applied in the airport environment.

For the purpose of this strategy paper, ACI EUROPE considers it essential to clarify how the term should be understood in the context of airports and hybrid threats.

At its core, critical infrastructure in the airport context should not be understood as a binary designation, but rather as a function of the airport's role in society.

This functional understanding of criticality does not replace or seek to redefine the formal designation of critical entities under the CER Directive[1] or national legislation. Rather, it reflects the strategic and societal role that airports may perform irrespective of their formal legal designation.

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Airports serve as strategic nodes within national, regional and European systems of mobility, connectivity and resilience. Their level of criticality is therefore determined not only by their size or traffic volume, but by their role in ensuring:

- connectivity of regions and countries
- continuity of essential supply chains
- support to emergency and crisis response
- military and strategic mobility
- societal and economic stability

This means that the criticality of airports varies significantly across Europe.

For example:

- In geographically isolated or island states, such as Malta, the airport represents a primary gateway to the outside world, making its continuous operation essential for national functioning.
- In larger and more diversified transport systems, individual airports may have more differentiated roles, where only certain functions are considered critical.

This leads to an important distinction:

Being a critical infrastructure does not necessarily mean maintaining full business continuity at all times, but rather the ability to ensure the continuity of functions that are essential to society.

In this context, ACI EUROPE proposes to distinguish between two dimensions of resilience:

2.1.1. Operational Continuity (Business Resilience)

The airport's ability to continue operating as a business entity, including:

- passenger and freight services
- commercial and other non-aeronautical activities
- operational efficiency

2.1.2. Critical Function Continuity (Societal Resilience)

The airport's ability to maintain or rapidly restore functions that are essential to society, including:

- safe and secure aircraft operations
- emergency and evacuation capabilities

- critical cargo and supply chain flows
- support to national and international crisis response

This distinction is important, as it allows airports and authorities to better prioritise resources and clarify expectations.

2.2. What Needs to Be Protected

In a hybrid threat context, the protection of critical infrastructure must go beyond physical assets and traditional security measures.

For airports, resilience depends on the protection of a broader set of functions, systems and dependencies that together enable the airport to fulfil its critical role.

These include:

2.2.1. Core Operational Functions

- Safe and continuous aircraft movements
- Airspace integrity and availability
- Ground handling and turnaround processes

2.2.2. Critical Systems and Technologies

- Air traffic-related systems (incl. GNSS-dependent functions)
- IT and OT systems supporting operations
- Communication systems
- Security screening infrastructure

2.2.3. External Dependencies

- Energy supply
- Telecommunications networks
- Navigation and surveillance infrastructure
- Fuel and logistics supply chains
- Access infrastructure (road, rail, etc.)

2.2.4. Organisational and Decision-Making Capability

- Crisis management structures
- Cross-functional coordination
- Ability to operate under uncertainty and ambiguity

2.2.5. Public Trust and Information Integrity

- Communication with passengers and operational stakeholders
- Ability to counter misinformation and panic
- Maintaining confidence in safe operations

This broader understanding is critical, as hybrid threats are often designed to target interdependencies, create uncertainty and disrupt systems indirectly rather than through direct attacks.

This understanding of critical infrastructure provides the foundation for how airports should be viewed in a hybrid threat context.

It shifts the focus from airport infrastructure as static assets to airport infrastructure as a set of critical societal functions.

Against this backdrop, it becomes essential to examine the role of airports not only as infrastructure operators, but as strategic nodes within Europe's wider resilience architecture.

3. Airports as Strategic Infrastructure within Europe's Critical Infrastructure Ecosystem

Airports are a central component of Europe's critical infrastructure ecosystem. They are not merely transport facilities, but strategic nodes for mobility, trade, economic activity, societal functioning and national and international connectivity.

As infrastructure hubs, airports connect people, goods, supply flows, national and international networks, as well as public and private functions. They also play an important role within national and European preparedness and response structures.

Airports are characterised by a high degree of complexity. They combine physical assets, digital systems, operational processes, security regimes and extensive stakeholder ecosystems within a single operating environment. This makes them efficient, but also vulnerable to interference designed to exploit complexity, dependencies and interfaces.

Airports also depend on a range of external and partially externally controlled systems and infrastructures, including:

- energy supply
- telecommunications and data networks
- navigation and surveillance systems
- road and public transport access

- water and technical utilities
- fuel and logistics chains
- digital service providers and third-party operators

These dependencies mean that airport resilience is not determined solely by what happens within the airport operator's direct control. In many cases, important vulnerabilities and dependencies extend beyond the physical airport perimeter.

Disruption affecting a single component can therefore have broader and faster consequences than previously assumed. Even incidents with limited physical scope may escalate into significant operational, economic or societal disruption if they affect critical functions, key systems or peak-demand periods.

This interdependence makes airports particularly relevant in a hybrid threat context. Hybrid tactics often seek not to maximise physical destruction, but rather to generate disruption, uncertainty, disproportionate effects, loss of trust, decision-making pressure and exploitation of organisational and technical grey zones.

This underlines the need to view airports as part of a broader critical infrastructure ecosystem, where resilience is not only about protecting individual assets, but about ensuring the ability to maintain, adapt and restore function under complex and dynamic conditions.

4. Understanding Hybrid Threats in the Airport Context

The term "hybrid threats" is increasingly used in European security and preparedness discussions, but in practice there are still significant differences in how it is understood and operationalised in the airport context.

This is not surprising. Airports operate in an environment where incidents are often managed according to their immediate nature and consequences rather than their strategic label. A drone incident, cyberattack, GNSS disruption or power outage will typically be managed operationally as a concrete event, regardless of whether it is later assessed as having a hybrid dimension.

This pragmatic approach is necessary and rational in an operational setting. However, it also makes it more difficult to develop a common, cross-cutting understanding of the overall threat environment and to build more mature organisational and strategic frameworks.

Hybrid threats in the airport context can be understood as coordinated, combined or mutually reinforcing actions across physical, digital, technological and information

domains, intended to create disruption, uncertainty, functional degradation or loss of trust — often with unclear attribution and outside traditional forms of conflict.

Hybrid threats typically exploit complexity and dependencies, cut across organisational and regulatory boundaries, combine multiple tools simultaneously or sequentially, create ambiguity regarding cause, actor and intent, and challenge decision-making under time pressure and uncertainty.

In practice, this means that hybrid incidents often cannot be fully managed through a single function or a single established procedure. Increasingly, they require cross-functional situational awareness, rapid coordination, robust governance, organisational flexibility and leadership maturity.

Existing aviation security, safety, cyber security, business continuity and crisis management structures remain essential foundations for airport preparedness and resilience. The challenge is not to replace these established structures, but to connect them more effectively when incidents cut across traditional organisational and regulatory boundaries.

This is precisely why hybrid threats in the airport context should be understood as a broader resilience issue rather than purely a security or cyber issue.

5. The Evolving Threat Landscape

The hybrid threat environment affecting European airports is clearly evolving. Whereas airports previously planned primarily around known and relatively bounded incident types, there is now growing recognition that future threats will be more complex, ambiguous and cross-border in nature.

Across Europe, airports are increasingly encountering — or preparing for — incidents that do not fit neatly into traditional categories, but instead combine elements from multiple domains at once. This includes physical, digital, technological and information-based forms of disruption.

A central feature of this threat environment is that many incidents are difficult to attribute quickly and conclusively. As a result, airports often need to protect operations and safety before it is clear whether an incident is caused by criminality, activism, system failure, opportunistic behaviour or more strategic interference.

That uncertainty is itself part of the hybrid challenge.

Hybrid threats affecting airports should not be understood as a fixed or exhaustive set of scenarios. Rather, they represent an evolving and adaptive threat environment.

While this paper provides examples of observed and emerging threat types, these should be understood as illustrative rather than comprehensive.

The defining characteristic of hybrid threats is precisely their unpredictability and ability to evolve, meaning that the next disruption may arise from vectors not yet identified or fully understood.

This requires airports, their stakeholders, policymakers and regulators to move beyond static threat models towards more adaptive and resilience-based approaches.

This evolving and increasingly complex threat landscape is not theoretical.

5.1. Drone Activity and Asymmetric Airspace Disruption

Drone activity around airports is now one of the most visible examples of asymmetric disruption with the potential to generate significant operational consequences using relatively limited means. For European airports, drone activity is not only a security issue, but also a matter of airspace integrity, operational continuity and crisis management. This is particularly evident where drone sightings or activity result in temporary airspace closures, cancellations, delays, diversions and resource-intensive verification and response efforts. The drone issue illustrates how low-cost tools can exploit highly critical environments and generate disproportionate effects.

5.2. Balloons and Low-Tech Cross-Border Disruption

In addition to drones, experience from the Baltic region shows that low-tech airborne objects — including balloons and so-called “weather balloons” — can also constitute a real challenge in a hybrid threat environment. In the eastern part of Europe in particular, there have been incidents involving objects drifting across borders — including from Belarus — generating uncertainty around airspace integrity, threat assessment and the required response. Such incidents matter precisely because they can be difficult to identify and classify quickly, create ambiguity regarding intent and risk level, may trigger operational restrictions or resource-intensive responses, and test coordination between airports, aviation authorities and national security actors. Balloons and other simple airborne objects illustrate that hybrid threats are not necessarily high-tech. On the contrary, their effect may lie precisely in being cheap, ambiguous and difficult to manage within existing categories.

5.3. Cyber Threats and Digital Pressure

Cyber threats are a persistent and growing challenge across European airports. As more and more critical functions become digitally enabled or digitally dependent, cyber increasingly becomes a matter of operational resilience rather than information security alone. Across the sector, this includes DDoS attacks, phishing and social engineering campaigns, third-party compromise attempts, and persistent efforts at digital intrusion or disruption. Cyber becomes particularly significant in a hybrid context when it is combined with other forms of disruption or targets systems and functions with high operational importance.

5.4. GNSS Jamming, Spoofing and Navigation-Related Disruption

Several European airports — particularly in geographies closer to the eastern edge of Europe — have experienced, or are actively preparing for, challenges linked to GNSS jamming and spoofing. This form of interference is especially challenging because it can occur relatively discreetly, is difficult to attribute quickly, may affect situational awareness and confidence in systems, and can generate operational friction without necessarily causing visible damage.

5.5. Physical Sabotage and Off-Airport Vulnerabilities

A key feature of the current threat environment is the growing recognition that many of the most critical airport vulnerabilities do not necessarily lie within the airport's own physical perimeter. Airports depend on a wide range of external infrastructures and technical connections, including energy supply, telecoms and data links, navigation and surveillance infrastructure, water and technical utilities, logistics connections and fuel supply. This makes it possible to affect airport functioning through attacks on peripheral or indirect components — a central feature of many hybrid approaches.

5.6. Human Factors, Insider Threats and Security Culture

The human dimension is an important element of hybrid resilience. Airports depend on large and diverse workforces, contractors, suppliers and third-party personnel, many of whom require legitimate access to operational areas, systems, information or infrastructure. This can create vulnerabilities through insider activity, social engineering, manipulation or the misuse of legitimate access.

At the same time, employees represent a key resilience capability. A strong security culture, appropriate awareness and trusted reporting mechanisms can help staff identify unusual behaviour, emerging vulnerabilities and weak signals before they develop into more serious incidents.

Hybrid resilience therefore requires attention not only to systems and infrastructure, but also to people, organisational culture and trusted reporting.

5.7. Disinformation, Social Media and Perception-Based Disruption

The information domain is playing a growing role in airport resilience. In a sector where public trust, passenger behaviour and timely communication are critical, misinformation, disinformation and digital mobilisation can have significant effects. This may include online mobilisation of protests or disruptions, the spread of misleading information during incidents, amplification of operational problems via social media, and pressure on management and authorities through perception-based influence.

5.8. Cascading and Multi-Domain Scenarios

The defining feature of the hybrid threat environment is not necessarily the individual incident types themselves, but the risk of combined and mutually reinforcing events. It is precisely at the intersection of:

- cyber and operations,
- drone activity and airspace management,
- external infrastructure and terminal operations,
- misinformation and crisis leadership, and
- technical disruption and public uncertainty,

that airport resilience is increasingly tested. This is what makes hybrid threats a governance and resilience challenge rather than a purely security challenge.

Across Europe, airports are already encountering many of these dynamics in practice.

The following section therefore outlines how airports are currently responding — and how resilience is being developed across the sector.

6. What Airports Are Doing Today

European airports are actively strengthening their resilience in response to an increasingly complex threat environment. However, the level of maturity, investment and organisational integration varies significantly across the sector.

This variation is closely linked to geographical exposure, threat perception and national security context. It also reflects differences in airport size, strategic role, available resources and existing capabilities. There is therefore no single level of maturity or response model across European airports, and resilience measures need to be proportionate and scalable.

6.1. Different Starting Points and Levels of Maturity

Airports located in regions with higher geopolitical tension, particularly in Northern and Eastern Europe, have in many cases developed more advanced resilience capabilities.

Exposure is not static. It can change rapidly, and airports that previously considered themselves low-risk may quickly find themselves in a different position.

The current European landscape is therefore characterised by different starting points and levels of maturity. This reinforces the need for approaches that can be adapted to the risk profile, role and capabilities of individual airports, including small and medium-sized airports.

6.2. Strengthening Technical and Operational Capabilities

Across Europe, airports are investing in:

- counter-drone detection and response capabilities
- enhanced perimeter awareness
- cyber security and incident response
- redundancy in critical systems
- improved operational resilience mechanisms

These investments reflect growing recognition that relatively simple means can generate significant operational consequences and that airports need capabilities that can support both prevention and continued operations during disruption.

6.3. Building Cross-Functional Governance and Situational Awareness

A clear trend is towards stronger integration within airport organisations and governance across:

- security
- cyber
- operations
- safety
- crisis management

Hybrid threats rarely manifest within a single domain.

Airports are therefore increasingly moving towards integrated operational models, where situational awareness and decision-making are shared across functions.

6.4. Scenario-Based Exercises and Adaptive Planning

Airports are increasingly conducting exercises that reflect:

- multi-layered incidents
- incomplete information
- simultaneous disruptions
- cross-functional decision-making

Hybrid incidents are not defined by a single event, but by the interaction of multiple disruptions.

This highlights the importance of:

- decision-making under uncertainty
- coordination with operational stakeholders and competent authorities
- rapid escalation mechanisms

6.5. Strengthening Cooperation with Authorities and External Partners

Airport resilience increasingly depends on effective cooperation beyond the airport organisation itself.

Effective coordination between airports, police, defence, aviation authorities and other relevant public authorities is particularly important where incidents extend beyond the airport operator's direct responsibilities or capabilities.

This cooperation is also relevant to external partners and service providers on which critical airport functions depend.

6.6. Emerging Practices and Lessons Learned

Several airports and national systems have developed advanced approaches that can serve as reference points for the wider sector.

Examples include:

Nordic countries (e.g. Norway, Finland)

- Strong integration between airports, police and defence
- High situational awareness linked to geopolitical exposure

United Kingdom

- Rapid scaling of counter-drone capabilities following major disruptions

- Integration of military support in crisis situations

France

- Early investment in advanced detection technologies
- Strong coordination between airport operators and state authorities

These examples demonstrate that:

- the sector is not starting from zero
- there is already valuable experience and capability available
- but knowledge-sharing and scaling of best practices remain limited

While these developments demonstrate significant progress across the sector, they also highlight important differences in maturity, capability and support.

The current landscape is therefore characterised not only by advancement, but also by fragmentation.

This leads directly to a set of structural challenges that continue to limit the overall resilience of European airports.

7. Key Challenges and Gaps

A number of structural and systemic challenges continue to constrain the overall level of resilience across the sector.

7.1. No Common Governance Model — and Often No Clear Owner

There is currently no single European model for how hybrid threats and resilience are organised within airports. Responsibility is distributed in different ways across security, operations, cyber, business continuity, risk, compliance and emergency management. These functions may each address individual elements of a threat while lacking a shared understanding of the wider, potentially multi-domain situation. The core need is therefore not necessarily organisational uniformity, but clear central decision-making capability, shared situational awareness and mature cross-functional governance.

7.2. Business Continuity Is Necessary — but Not Sufficient

Many airports have relatively mature business continuity and contingency arrangements. But hybrid incidents are often more ambiguous, more simultaneous, more cross-domain, more dependent on external actors, and harder to reduce to fixed procedures. A broader resilience approach is therefore needed — one that also includes leadership, governance, adaptation, situational awareness and recovery under uncertainty.

7.3. Information Provided by State Authorities Remains Inconsistent and Often Insufficient

One of the most significant and recurring challenges across the sector concerns the relationship with public authorities in terms of information-sharing and support. Many airports experience a mismatch between the requirements placed upon them, the threat awareness they are expected to act on, and the information they actually receive in time and in usable form. Viewed across Europe, information provided by state authorities remains one of the most important maturity gaps.

7.4. Existing Frameworks Are Not Sufficiently Aviation-Specific

Many existing European and national frameworks relating to critical infrastructure, cyber resilience, preparedness and societal security remain too generic for the specific realities of airports. Airports are open and complex environments, multi-actor systems, highly regulated, strongly dependent on external infrastructures, and carriers of security, societal and mobility functions at the same time. This requires a much stronger aviation-specific interpretation and operationalisation.

7.5. Funding and Cost-Sharing Remain Unresolved

When airports are expected to invest in counter-drone capabilities, cyber resilience, redundancy and backup, exercises and preparedness, monitoring and situational awareness, as well as protection of off-airport dependencies, a legitimate question arises: who should pay for protection against strategic hybrid threats with potentially society-wide consequences? Without greater clarity, Europe risks developing an uneven resilience landscape.

7.6. A Common European Framework Is Still Missing

Across the sector, there is a growing recognition of the need for a common language and shared understanding, practical governance models, better sharing of experience and lessons learned, more systematic cooperation across airports and authorities, and a stronger collective European voice. This is precisely the space in which ACI EUROPE has an important and natural role to play.

8. Way Forward – 5 Key Principles

ACI EUROPE considers that hybrid threats affecting European airports constitute a structural and enduring strategic challenge to Europe's wider critical infrastructure ecosystem and societal resilience.

These threats are no longer emerging. They are already materialising across the European aviation system, as demonstrated by recent incidents involving drone disruption, GNSS interference, cyber pressure and cross-border activity.

ACI EUROPE also considers that hybrid threats cannot be addressed adequately within traditional and separate categories such as aviation security, cyber security, safety, business continuity or crisis management alone. While each of these disciplines remains essential, it is increasingly the interaction between them that defines the real resilience of a modern airport.

Across European airports, there is a clear movement towards a more integrated understanding of resilience, focused not only on prevention and protection, but equally on the ability to absorb disruption, maintain critical functions under pressure, adapt to complex and ambiguous events, and restore operations and trust quickly and safely.

The examples discussed in this paper show that even limited or low-cost actions can generate disproportionate operational and societal effects.

This underlines that hybrid threats are fundamentally about exploiting systemic vulnerabilities — not about isolated attacks.

ACI EUROPE therefore considers that Hybrid Threats and Airport Resilience should be addressed as a strategic issue of leadership, governance and societal resilience.

8.1. Hybrid Threats Against Airports Must Be Recognised as a Strategic Critical Infrastructure Issue

ACI EUROPE believes that hybrid threats affecting airports should not be treated as a niche or sub-sector issue, but as a strategic challenge for Europe's wider critical infrastructure ecosystem and societal resilience.

8.2. Airport Resilience Must Be Approached as an Integrated, Cross-Functional Capability

ACI EUROPE believes that effective management of hybrid threats requires stronger cross-functional governance, better central decision-making capability, and closer integration between existing functions and structures.

8.3. State Support and Operationally Useful Intelligence Are Essential

Without timely, actionable and operationally relevant intelligence from public authorities, airports are effectively required to manage state-level threat dynamics with incomplete situational awareness.

8.4. Existing Policy and Regulatory Frameworks Must Better Reflect Airport Realities

ACI EUROPE believes that future European and national frameworks for hybrid resilience should be more aviation-specific, operationally relevant, proportionate and compatible with existing aviation regulation and governance.

8.5. Hybrid Resilience Requires Structural Investment and Clearer Cost-Sharing Principles

ACI EUROPE considers that strengthening airport resilience against hybrid threats requires greater clarity on which capabilities can reasonably be expected from airports, which should be provided or supported by the state, and how investment in hybrid resilience should be financed and allocated proportionately.

9. Policy Recommendations

The developments discussed in this paper show that hybrid threats are already affecting operations, decision-making and resilience across the sector.

Incidents involving drone disruption, GNSS interference, cyber pressure and cross-border activity illustrate that even relatively limited actions can generate significant operational and societal consequences.

These developments underline the need for a more structured, coordinated and forward-looking policy response at European and national level.

9.1. Recommendations to EU Institutions

- Recognise hybrid threats against airports as a strategic European critical infrastructure issue.
- Better integrate airport-relevant hybrid scenarios into EU policy and regulatory frameworks.
- Establish a regular EU-level airport resilience dialogue between the European Commission, Member States and airport operators, using ACI EUROPE as the sector interface to share threat developments, operational lessons and good practices.
- Make airport hybrid-resilience projects eligible for relevant EU security, resilience and research funding, and encourage Member States to provide complementary national funding for operational capabilities.
- Develop EU guidance for hybrid incidents affecting airports that aligns reporting and information flows across aviation security, aviation safety, NIS2 and CER frameworks, and establishes a clear national coordination mechanism between the competent authorities so that airports are not required to report the same incident through multiple unconnected channels.

9.2. Recommendations to National Governments and Authorities

- Provide airports with timely, actionable and operationally relevant intelligence.
- Clarify roles, responsibilities and escalation mechanisms for hybrid incidents affecting airports, recognising the limits of airport operators' mandates, capabilities and resources. Establish clear thresholds and procedures for intervention by competent state authorities where threats exceed those limits, ensuring a timely and coordinated response while airport operators continue to manage operational safety and continuity.
- Apply the point to specific threats, including drones, through clearly defined national arrangements for detection and response developed in cooperation with airport operators. Responsibility for counter-drone interception or neutralisation should rest with competent state authorities
- Integrate airports appropriately into national critical infrastructure and resilience strategies.
- Develop clearer principles for funding, cost-sharing and state support where airports are expected to address strategic or state-level threats, including removing unnecessary legal or procurement barriers that may prevent airports from acquiring the capabilities required to fulfil their responsibilities.

9.3. Recommendations to Airport Operators

- Strengthen cross-functional governance and central decision-making capability for hybrid threats and resilience.
- Develop and regularly exercise scenario-based planning for complex, ambiguous and multi-domain incidents.
- Map and address critical external and third-party dependencies, including external infrastructure, digital service providers, critical suppliers, contractors and other third parties whose disruption or compromise could affect critical airport functions.
- Strengthen awareness, monitoring and organisational learning, including attention to human factors, insider threats, security culture and trusted reporting mechanisms.

10. Conclusion

Hybrid threats are not a temporary or peripheral challenge for European airports. They are part of the new operational reality that airports increasingly need to strategically, organisationally and operationally address.

The key question is therefore no longer whether European airports should prepare for hybrid threats, but how Europe as a whole will ensure that they are able to do so effectively, proportionately and in close cooperation with the authorities and institutions that share responsibility for protecting critical infrastructure.

ACI EUROPE believes that the time has come to move work on Hybrid Threats and Airport Resilience from a fragmented and partly reactive level to a more mature, coordinated and forward-looking European approach.

European airports are already moving in that direction. The next step must be to ensure that the political, regulatory and cooperative frameworks evolve at the same pace as the threat itself.

ACI EUROPE is the European region of Airports Council International (ACI), the only worldwide professional association of airport operators. ACI EUROPE represents over **600 airports** in **55 European countries**. Our members facilitate over **95% of commercial air traffic** in Europe. Air transport supports **14 million jobs**, generating **€851 billion** in European economic activity (**5% of GDP**). In response to the Climate Emergency, in June 2019 our members committed to achieving Net Zero carbon emissions for operations under their control by 2050, without offsetting.

EVERY FLIGHT BEGINS AT THE AIRPORT

For more information, please contact:
Sébastien Colmant
Director of Aviation Security and Cyber Security
sebastien.colmant@aci-europe.org

www.aci-europe.org
ACI EUROPE

© Copyright ACI EUROPE 2026

