Cyber-Air Security in Civil Aviation: Rising Threats and the Road to Resilience

Mona Al Achkar Jabbour

Permanent Member of the data security Panel - Erice

Presented at the ICAO/UNOOSA Symposium, August 28–31, 2017

Every day, millions of passengers board aircraft with an expectation that extends far beyond on-time arrivals and comfortable seats: they expect to be safe. Aviation safety has long been understood in physical terms, preventing hijackings, screening for weapons, securing perimeters. But as commercial aviation has become increasingly dependent on networked digital systems, a new and urgent dimension of security has emerged. Cyber threats to civil aviation are no longer theoretical; they are here, they are escalating, and the industry's legal, technical, and regulatory frameworks have yet to fully catch up.

This article draws on research presented at the ICAO/UNOOSA Symposium in 2017 by Mona Al Achkar Jabbour of Lebanese University and the Pan-Arab Observatory for Cyber Security. Her analysis charts the scope of the cyber threat in civil aviation, reviews landmark incidents, examines the evolving international regulatory response, and lays out a comprehensive framework for a more secure aviation future.

Redefining Aviation Security for the Digital Age

Traditional aviation security focuses on preventing unlawful physical interference with aircraft, acts such as seizure, destruction, hostage-taking, forcible intrusion, or the introduction of weapons and hazardous materials. These remain critical concerns. But cybersecurity adds a fundamentally different dimension: the protection of the integrity of networks, programs, and data from attack, damage, or unauthorized access. Crucially, it also encompasses resilience and survivability, the ability of systems to continue operating, or recover quickly, even after an attack.

The two domains are increasingly intertwined. A cyber attack on aviation is not merely a matter of data compromise, it can disable physical systems, endanger aircraft, and cost human lives.

A Rapidly Changing Threat Landscape

The civil aviation sector has undergone a profound digital transformation. The widespread adoption of interconnected systems, Commercial Off-The-Shelf (COTS) software, and next-generation cockpit technologies, which allow pilots to synchronize

flight information with external networks, has dramatically expanded the attack surface. Air Traffic Management (ATM) systems, which once operated in relative isolation, now depend on sophisticated digital infrastructure subject to the same vulnerabilities as any networked system.

The Internet of Things (IoT), cloud computing, big data analytics, artificial intelligence, and cognitive systems have brought genuine operational efficiencies. But they have also introduced new and novel threats, new vulnerabilities, and a rising level of systemic risk complexity. Every new connected device added to the aviation ecosystem represents a new potential entry point for an attacker.

Three categories of systems face the greatest exposure: internal airport computer systems, in-flight aircraft control systems, and air traffic management systems. Cyber attacks against these systems can directly affect civil aviation in the physical domain — disrupting flight schedules, blocking communications between cockpits and control centers, manipulating flight data, or causing outright data loss. Any physical connection that passes data is a potential pathway for an attacker, including maintenance systems, radio links, and the platforms that connect operators with aircraft.

Incidents That Changed the Conversation

The abstract risks of aviation cybersecurity have been made concrete by a series of real-world incidents. In 2006, the US Federal Aviation Administration was forced to shut down air traffic control systems in Alaska following a network breach. Three years later, in 2009, another attack on FAA computer systems resulted in hackers accessing personal information on approximately 48,000 past and present employees, and raising fears about what further penetration of operational systems could have meant.

Perhaps the most sobering case came from Spain. The crash of Spanair flight 5022 in August 2008 killed 154 people. The Civil Aviation Accident and Incident Investigation Commission of Spain determined that the aircraft's central computer system, used for monitoring technical problems on board, had been infected with malware. While investigators cited multiple contributing factors, the malware's presence in a critical monitoring system illustrates the lethal potential of compromised aviation software.

In 2013, a cyber attack caused the shutdown of passport control systems at Istanbul's Atatürk and Sabiha Gökçen airports, delaying numerous flights and demonstrating how even support-level infrastructure, when compromised, can cascade into significant operational disruption.

The Democratization of Danger

What makes the current cyber threat environment particularly alarming is the democratization of attack capability. Cyber weapons are no longer the exclusive province of government agencies and elite hackers bound by professional ethics. Sophisticated exploits, some stolen from intelligence agencies, others available for purchase on dark web markets, can now be wielded by rogue nation-states, criminal

organizations, and lone actors operating on minimal budgets from virtually anywhere in the world.

The goals of such attacks vary: stealing confidential or sensitive information, manipulating or erasing data, seizing control of systems or services, or causing direct physical damage. The potential consequences for aviation range from limited operational disruptions to, in worst-case scenarios, loss of aircraft control, making cyber nihilism a genuine strategic concern.

To date, most documented attacks have targeted support functions rather than core operational systems. But the trajectory is worrying. Time surveillance systems, communications, and flight information networks, the operational backbone of civil aviation, remain at risk. State-sponsored actors have been identified in multiple reports, and the blurring of lines between defensive cybersecurity and offensive cyber attack raises urgent questions for international law and diplomacy. Events such as the Stuxnet malware campaign demonstrated that digitally-delivered weapons can cause real physical damage to industrial infrastructure , a warning the aviation sector cannot afford to ignore.

The International Legal Framework: Progress and Gaps

The international community has been slowly adapting its legal frameworks to address the cyber dimension of aviation security, but significant gaps remain. ICAO adopted Annex 17 in the early 1970s to help member states prevent unlawful interference in aviation, but cyber threats were long left unaddressed. The Chicago Convention on Civil Aviation continued to treat cybersecurity as a recommended practice rather than a binding standard.

An important step forward came with Chapter 4 of Annex 17, which now mandates that each contracting state develop measures to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize safety. ICAO was also developing new safety standards for 2018 concerning large unmanned aircraft capable of crossing borders.

The Beijing Convention of 2010 was hailed as the first significant step in securing the aviation industry against modern threats. It criminalized using civil aircraft as weapons and the use of dangerous materials against aircraft or ground targets. Cyber threats were addressed implicitly: communicating false information that endangers an aircraft in flight constitutes an offense under the Convention, applicable to interference with air navigation services. However, the phrase 'in flight' may limit the Convention's scope in certain scenarios, for instance, when interference occurs while aircraft doors are still open.

The April 2017 Dubai Declaration on Cybersecurity in Civil Aviation marked a meaningful political commitment. States affirmed their responsibility to mitigate cyber threats, build national capacity to address them, and ensure that domestic legislative frameworks can hold cyber attackers accountable. The Declaration held that cyber capabilities applied to aviation must be used exclusively for peaceful purposes, and that

inter-state collaboration is an essential precondition for any effective global framework. Crucially, it called for universal ratification of the Beijing Instruments, noting that their entry into force would make a cyberattack on international civil aviation a recognized criminal offense and serve as a meaningful deterrent.

A Framework for Mitigation

Addressing the cyber threat to civil aviation requires action across four interconnected pillars: awareness and capacity building; collaboration between stakeholders; robust legislation, regulation, and standards; and structured information exchange.

Cyber protection in aviation is an inherently shared responsibility. Governments, airlines, airports, manufacturers, and international bodies all have a role to play, and none can succeed in isolation. The private sector, with its intimate knowledge of its own systems and vulnerabilities, should lead in developing new security regimes, while government brings complementary resources: financial support, regulatory authority, and the ability to coordinate across private actors who might otherwise operate in silos.

Regulatory frameworks must be both specific and general: specific enough to address the particularities of civil aviation, while broad enough to account for the fact that aviation technologies are shared with other critical infrastructure sectors. A framework calibrated only for generic critical infrastructure will miss aviation-specific vulnerabilities; one that fails to connect with wider national infrastructure protection plans will leave dangerous gaps.

Sector-based risk assessments should inform regulation, with legislation designed to harmonize multi-stakeholder efforts, support public-private collaboration, and foster mutually agreed solutions. Regulation must avoid creating unbalanced frameworks across different world regions, inconsistency invites exploitation.

The Case for Proactive Law

One of the most compelling arguments in this analysis is the call for a proactive approach to law, one that does not merely react to incidents but anticipates the nature and evolution of technology-driven risks. In civil aviation, virtually every function, such as engineering, management, operations, and maintenance, is conceptualized around the use of information and communications technologies. Accordingly, law must be designed around this reality, not retrofitted to it after the fact.

Existing legal building blocks where we find air law conventions, cybercrime treaties, data protection regulations, and directives such as the EU Network and Information Security (NIS) Directive, are providing the foundation, but they were not designed with aviation cybersecurity as a central concern. Hence the question is not whether these tools are useful, but whether they are sufficient.

Proactive law is not merely about drafting statutes in advance of disasters. It means using legal tools to shape future behavior: organizing internal controls, defining the roles and responsibilities of all parties in the civil aviation ICT ecosystem, establishing

liabilities and obligations across administration and operations, and committing nation-states to the ongoing governance of shared digital infrastructure. It also means building legal literacy into the sector's culture in order to help aviation organizations and their personnel stay ahead of legal risk rather than scrambling to manage it after a breach.

Technical Imperatives

On the technical side, the approach to aviation cybersecurity must evolve from static perimeter defense to dynamic, layered resilience. This means combining defense-in-depth strategies with advanced threat detection and mitigation capabilities, shifting from simply walling off systems to actively monitoring, detecting, and responding to attacks in real time.

An important strategic insight concerns Advanced Persistent Threats (APTs) sophisticated, targeted attacks that are currently a minority of total cyber threats but represent the most dangerous category. Preparing defenses against APTs inherently strengthens protections against more common threats as well, since common attack trajectories are often early steps in more complex APT methodologies. Investing in worst-case defenses thus yields broad-spectrum protection.

Cyber defense testing should be integrated into the airworthiness certification process itself and shall be treated not as an optional audit but as a fundamental condition of safe operation. The industry should adopt security by design, embedding cybersecurity into the architecture of aviation systems from the earliest stages of development rather than bolting it on afterward.

The Way Ahead

The path forward requires a concerted effort on multiple fronts simultaneously. At the national level, states must enact legislation that clearly defines how civil aviation sector assets are protected and how cooperation between the public and private sectors is organized. At the international level, the priority is to close the current gaps: stopping emerging information threats, building mutual trust between stakeholders, and constructing governance frameworks on the foundation of international, regional, and national agreements.

The concept of a 'digital Chicago Convention' providing international cyber provisions for aviation analogous in ambition and scope to the 1944 Convention on International Civil Aviation, offers a compelling vision. Just as the original Chicago Convention established the foundational norms for the safety and sovereignty of international air travel, new digital provisions could set binding standards for cybersecurity across the entire civil aviation system, creating a common regulatory culture that enables mutual recognition and a converging understanding of emerging threats.

Practical steps include establishing national and international centers for cybersecurity in aviation, developing performance metrics to measure the effectiveness of cyber risk mitigation, issuing cybersecurity certificates that attest to compliance with agreed

standards, and building the information-sharing infrastructure that allows threats identified in one part of the system to protect the whole.

Resilience and cyber survivability, which is considered to be the capacity to maintain operations and recover from attacks, must be treated as core design objectives, not afterthoughts one.

Conclusion: Making Cybersecurity Part of Aviation's DNA

Civil aviation is one of humanity's most complex and significant technological achievements, a global system that moves over four billion passengers a year and underpins international commerce. Its digital infrastructure is both its greatest operational asset and its most significant emerging vulnerability.

The threat is real, it is growing, and it does not respect borders. The incidents already on record, from FAA network breaches to the Spanair disaster are warnings. Defenders in the aviation sector have the advantage of knowing what is coming. The question is whether governments, regulators, industry, and the international community can move fast enough, and work together closely enough, to build defenses commensurate with the threat.

Achieving that requires more than technology. It requires a fundamental shift in organizational culture, legal architecture, and international cooperation making cybersecurity not a compliance checkbox but an intrinsic part of how civil aviation is designed, operated, regulated, and governed.

let us be cyber alerted, and make cybersecurity part of the sector's DNA.