



# AVIATION CYBERSECURITY

## Finding Lift, Minimizing Drag

### REPORT OVERVIEW

**By creating a mutual understanding of cybersecurity that everyone can benefit from, and one that the public, policy makers and leaders in our own community can support, we will help assure resiliency.**

#### Alan Pellegrini

CEO, Thales North America  
Board member, Atlantic Council

Today, the aviation community is benefitting from new levels of digitization and connectivity. These technological advancements are creating tremendous opportunities for flight efficiency, customer service, security, operations and the passenger experience—both in the air and on the ground. Yet, with new levels of efficacy gained by increased digitization and connectivity, new levels of vulnerability also arise.

A 2017 report by the Atlantic Council marked an important step in creating awareness and helped drive needed public dialogue on cybersecurity in aviation. Starting this dialogue to strengthen the community's resilience in the face of new cyber realities is the reason Thales chose to underwrite the Atlantic Council report, which promises to create a foundation for how the community can come together to protect the traveling public.

Anticipating, identifying, and mitigating cyberspace vulnerabilities in the aviation community is a significant challenge and one that must be confronted by every stakeholder—not just the largest or most visible.

#### PRIORITIES

- **Encourage a dialogue among aviation leaders about the realities, benefits and risks of aircraft system digitization and connectivity.**
- **Engage multiple industry, infrastructure and supply chain stakeholders to identify priorities for threat defense, mitigation and prevention.**
- **Increase industry and government transparency regarding effective strategies for cyber resilience and evolving threats.**

The industry's diverse stakeholders—airlines, airports, air traffic management, and other critical stakeholders—must continue to examine the issue from a broader perspective, which is essential to community-wide strength and security. Even the smallest aviation cybersecurity incident can have major cascading impacts if public trust is broken because of a uniquely inter-reliant ecosystem.

By generating a mutual understanding of cybersecurity, one that the public, policy makers, and leaders in our own community can embrace, we will help assure a stronger, safer future. When it comes to the trust of travelers and the prosperity of the community, we are all only as strong as our most vulnerable enabler.

Thales will continue to lead this important dialogue, because there are many ways we can fail and only one way we can succeed—through the engagement and commitment of the entire aviation community.

## Foundations of Aviation Cyber Safety and Security

#### GOVERNANCE & ACCOUNTABILITY

Top-down leadership required to secure weak links in the system.

#### SYSTEM RESILIENCE

Global approach required to balance security and resiliency.

#### STAKEHOLDER TRUST

The aviation ecosystem must consider the challenge of building public/stakeholder trust in tandem with cybersecurity challenges.

#### SECURED DECISION-MAKING

Informed, timely human decisions must be protected from the risk of data integrity attacks and adversary subversion.

#### SHARED PERSPECTIVE AND CULTURE

A "cultural exchange" between cyber and aviation industries must be encouraged.



**It is crucial that all the stakeholders along the supply chain espouse a collaborative and risk-informed cybersecurity framework to strengthen the resilience of aviation systems against attacks.**

**Deborah Lee James**  
Former secretary of the Air Force  
Board member and fellow, Atlantic Council

While the aviation sector has grown in scale and profitability over the past decade, the enterprise Information Technology (IT) it depends on is proving undependable, disrupting operations even in the absence of adversaries. Policy and industry leaders across both aviation and cybersecurity are working toward regulation and standardization but face a significant challenge due to the speed of industry and adversary innovation.

**IMPACT OF SYSTEMIC FAILURES**

Non-cyber failures demonstrate how quickly incidents can rapidly cascade and disrupt operations. Risk should be a key motivator for the aviation industry to not just improve cybersecurity but to collaborate across systems.

**AVIATION IS BECOMING A BIGGER TARGET**

Increasing technology and connectivity has brought new opportunities for malicious actors to target the aviation industry. Industry has decades of experience in preventing safety and security issues, but the cybersecurity and cyber safety challenge is comparatively novel.

**THE CONNECTED AIRCRAFT**

Connectivity of aircraft systems—through traditional information technologies, aviation-specific protocols, and RF communication—has extended the attack surface to the aircraft itself, whether on the ground or in flight.

**MANUFACTURING AND SUPPLY CHAIN**

As technology radically transforms design, production, operation, and maintenance of aircraft, models of safety and security must change to keep alignment and demonstrate their efficacy to the public.

**AIR TRAFFIC MANAGEMENT**

Investments in ATM are already paying dividends in safety, environment, airport, flight operations, and financial returns. Many next generation ATM concepts evolved when technically capable and motivated adversaries were understandably not accounted for.

**AIRPORTS**

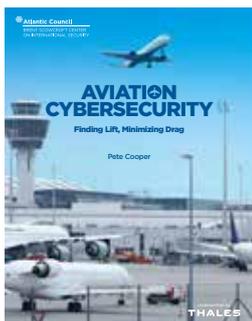
Airports are federations of several distinct organizations with potentially disparate approaches to governance, risk, compliance, and operations—yet the cybersecurity of one can affect all others.

**INDUSTRY COOPERATION: AVIATION & CYBERSECURITY**

Aviation and cybersecurity domains increasingly overlap, and the common goals of safety, resilience, and trust can be achieved sooner by working together.

**POLICY & REGULATION**

While national and international policies and regulations are unified for safety and physical security, it is yet unclear how aviation cybersecurity can achieve the same maturity and clarity.



**To view and download the full report, visit:**  
<http://aviationcyber.atlanticcouncil.org>