Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

AVIATION CYBERSECURITY

Finding Lift, Minimizing Drag

Pete Cooper

Underwritten by
THALES

AVIATION CYBERSECURITY

Finding Lift, Minimizing Drag

Pete Cooper

ISBN: 978-1-61977-397-4

November 2017

Contents

Foreword

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.

The launch of this report by the Atlantic Council marks an important step in creating awareness because it will help 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 this 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.

I applaud the Atlantic Council for bringing many diverse stakeholders to the table—airlines, airports, air traffic management, and other critical stakeholders—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 unlike any other.

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.

I hope we can challenge each other to continue to improve because there are many ways we can fail and only one way we can succeed—through the engagement and commitment of the whole community.

Sincerely,

Alan Pellegrini
CEO, Thales North America
Board member, Atlantic Council

Introduction

The aviation industry is currently experiencing a season of unprecedented change: one that demands careful balancing of cost with evolving business imperatives, customer demands, and safety standards. The increasing use of new technologies in the movement towards automation has yielded efficiencies and enhanced the customer experience. Yet, it has also inadvertently created vulnerabilities for exploitation. As a central component of commerce, trade, and transportation infrastructure the aviation industry is indispensable for the global economy. The consequences of failure would carry direct public safety and national security implications.

The complexity of the aviation ecosystem, with its many stakeholders, makes understanding the new nature of risk particularly challenging. How does the United States and its partners ensure that aviation remains a stable and secure environment as innovative technologies are integrated to ease congestion and meet demand?

Pete Cooper, a senior fellow at the Atlantic Council's Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security and author of Aviation Cybersecurity—Finding Lift, Minimizing Drag, speaks to the reality of cybersecurity. That while strong preventive measures may act as deterrence, declarations of fully secure systems are unrealistic. It is his belief that generating shared perspectives, leadership, and resilience in both systems and consumer trust are the keys to managing risk across the industry.

At present, there is an absence of clear or strong foundations in aviation cybersecurity to adequately prepare for and counter emerging threats across aircraft, unmanned aircraft systems, air traffic management, airports, and their supply chains.

Without a unified understanding and approach to these threats, coherent aviation cybersecurity may potentially struggle and risk failure. 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. This report helps to remedy the gap in perception of risk and recommend a nuanced strategy for the industry moving forward.

As the former Secretary of the Air Force, I know the importance of building reliable aerial systems and see the need for international dialogue in paving the way forward. Aviation cybersecurity will be as challenging as it is essential, and this report is initiating an important conversation to lead us in the right direction. Reading this Atlantic Council report is where all industry and government leaders should begin.

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

Executive Summary

This is a boom time for the aviation industry. The ten-year average for passenger growth hovers around 5.5 percent globally, aviation accidents and incidents are down to their lowest levels, profits are up due to historically low oil prices, and the increasing use of technology is transforming efficiency and passenger experience.[1] As an "always on" generation of travelers demand to be "always connected," an increasingly interconnected aviation industry is employing evermore digital technologies to deliver efficiencies: across aircraft (including Unmanned Aircraft Systems [UAS]), Air Traffic Management (ATM), airports, and their supply chains.

Aviation is a cornerstone of national and international commerce, trade, and tourism, which means even an isolated incident could spark a crisis of confidence in the entire sector. The potential impacts on stock market value, stability, and national gross domestic product make securing and protecting the connected aviation world a critical element of national security.

This study indicates that the aviation industry will likely experience cybersecurity challenges similar to other industries that have embraced the "digital revolution." As the industry moves forward, will it be able to maintain stakeholder trust by accurately perceiving the risks and opportunities as well as understanding adversary threats?

Previously, aviation systems were relatively secure due to the bespoke nature of their design, isolation from other systems, and little in the way of communication protocols. But ATM is no longer isolated, and ground services and supply chains are becoming fully integrated into an interconnected digital world.

In addition, cyber adversaries and their capabilities evolve and adapt quickly. This may be particularly challenging for an industry where many of the systems have long design and development periods. As technology radically transforms design, production, operation, and maintenance of aircraft, models of safety and security must adapt. While new and emerging capabilities, like additive manufacturing and UAS, are transforming the aviation sector, their novelty may obscure the cybersecurity risks these technologies introduce.

Connectivity of aircraft systems, through traditional information technologies and aviation-specific protocols, has now extended the attack surface to the aircraft itself. Aircraft are now complex data networks, yet the ability to monitor them arguably lags behind comparable ground-based networks—as does the ability to avoid and respond to potential cybersecurity incidents. ATM is also undergoing a sweeping modernization program that shifts away from legacy radars and beacons to a heavy reliance on Global Positioning Systems (GPS) and digital communications. Advanced technologies such as GPS and Automatic Dependent Surveillance—Broadcast (ADS-B) can greatly improve accuracy and reliability under normal conditions, yet remain susceptible to degradation by environmental hazards or manipulation by hostile actors.

Airports are a key focal point of adversary interest. As a federated management system with numerous interdependent service providers, deficiencies in airport cybersecurity may allow bypass, subversion, and eventual breaches of physical security. Additionally, as capabilities such as remote tower services gain popularity, balancing commercial interest with sound risk management will be even more difficult. Attacks against public-facing systems at airports may pose little safety risk, but can harm public confidence and trust.

As the domains of aviation and cybersecurity increasingly overlap, the common goals of safety, resilience, and trust can be achieved sooner by working together. Preserving aviation's strengths relies on clear definition of governance and accountability and recognition of shared responsibility across the supply chain. The aviation industry has a longstanding and robust safety management system with a safety culture embedded at its core.

The challenges of cybersecurity are testing these existing industry policies and frameworks as nations, organizations, and businesses attempt to develop best practices. There will be a key role for the International Civil Aviation Organization (ICAO) in bringing both leadership and vision to the challenge. With multiple perspectives and stakeholders, it is essential for the increasingly

1 "Another Strong Year for Air Travel Demand in 2016," IATA, press release, February 2, 2017, http://www.iata.org/pressroom/pr/Pages/2017-02-02-01.aspx.

Airliners holding for departure. *Photo credit:* Phillip Capper/Wikimedia.

interconnected aviation industry to have a clear, coherent vision.

A cybersecurity vision for a connected aviation industry and its foundation

A vision or aspirational state for the aviation industry as it faces cybersecurity challenges may be characterized as:

> *A safe and prosperous aviation industry with resilient trust and systems.*

To achieve this vision, the industry must focus on strengthening five foundations of aviation cybersecurity:

1. Systems Thinking, Governance, and Accountability

In a complex, interdependent, system of systems, finding and securing the weak links are not only an essential requirement but also a critical test of governance and accountability. The ICAO plays an important role in working with national regulators to decide how the aviation industry should manage cyber risks and to clarify and simplify the legislative burden for stakeholders.

2. Resilient Systems

"Advanced adversaries will still breach the IT infrastructure."[2] This assumption of future breach, failure, or attacks on data integrity has resulted in a greater focus to deliver resiliency as well as security. It will require both resilient systems engineering practices and a resilient personnel culture to safely work through such adversary activity.

3. Resilient Trust

The importance of stakeholder trust is at the forefront of the aviation cybersecurity challenge. If adversaries can erode trust, they are able to control passenger and stakeholder experience, perspective, and confidence. The longer it takes for an operator to counter perceptions and regain trust, the less credibility the operator will have in the eyes of the stakeholder.

2 Deb Bodeau and Richard Graubart, "Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls," Mitre, 2013, https://www.mitre.org/sites/default/files/publications/13-4047.pdf.

4. Secured Human Decision-Making

Human error or technical failure is inevitable, but all aviation systems are designed to help a human operator recognize and deal with an accident or incident before it impacts safety. Therefore, there must be a focus on protecting the integrity of the data that operators are presented with so they are able to make safe and timely decisions.

5. Shared Perspective and Culture

The importance of collaboration cannot be underestimated. Even beyond sharing knowledge and different perspectives, there is great potential for cultural exchange between the aviation and cybersecurity industries. Developing a shared culture in which both groups synergize and view the challenges and potential solutions will increase awareness of risk and robust resilience.

Suggested Next Actions

To build and fortify the aforementioned foundations, it is recommended that all stakeholders take the following actions:

- Reinforce Leadership and Standardization (Globally, Nationally, Regionally, etc.)
- Define a Common Understanding of Aviation Cyber Safety and Security
- Reevaluate, Develop, and Use Robust Threat Models
- Develop and Communicate Coherent Messaging on Cybersecurity Risks
- Find Ways to Develop Trust with Non-Technical Audiences
- Improve Agility in Security Updates
- Design Systems and Processes to Capture Cybersecurity-Relevant Data
- Train for Safety Across Multiple Disciplines
- Incorporate Cyber Perspectives into Accident and Incident Investigations

As organizations seek to exploit the opportunities of a connected aviation industry, they must retain the ability to be objective about both the benefits and risks. Innovative, connected technologies, if sympathetically and securely integrated, can assist in efficiency and safety; but this must not be at the cost of unknown or unacceptable risk.

It will take consideration and incorporation of multiple stakeholder perceptions to reduce the risk posed by adversaries. In a rapidly evolving environment, the industry must exercise leadership and utilize teamwork to boldly look to the horizon with clear purpose and maintain stakeholder unity. The conditions are ripe to find alignment, direction, and progress under strong international leadership to ensure a safe and thriving aviation industry in the years to come.

Acknowledgements

First, to the leaders below, as well as the many off-the-record contributors. The latter group includes perspectives from individuals across cybersecurity research, academic and pilot communities, as well as industry seniors representing technology companies, consultancies, manufacturers, airlines, and airports.

Second, to Thales for underwriting this report. Their energy, commitment, and collaboration demonstrated a great spirit of partnership. The Atlantic Council looks forward to working together on aviation cybersecurity in the future.

And third, to the members of the Atlantic Council's Brent Scowcroft Center on International Security. In particular, special thanks go to Priscilla Kim, Diya Li, Anni Piiparinen, Safa Shahwan, and finally Beau Woods for his insight, research assistance, and co-ordination of the project.

Kevin Borley – Consulting CIO, KJB Associates Ltd

Scott Buchannan – Federal Lead, Aviation Cyber Initiative, Department of Homeland Security

Sol Cates – Vice President of Technology Strategy, Office of the Chief Technology Officer, e-Security, Thales

Francois Delille – Director of Business and Product Strategy, Air Traffic Management, Thales

Mike Gadd – Business and Technical Lead, UAS & Cyber Programmes, UK Civil Aviation Authority

Philippe Jasselin – Cybersecurity Development Manager, Air Traffic Management, Thales

James Holland – Head of Aviation Safety, 1 Group, UK Royal Air Force

Steve Luczynski – Former Deputy Director for Cyber Plans and Operations, US Department of Defense

David McCamley – Policy Specialist, Airspace and Air Traffic Management, UK Civil Aviation Authority

Sam Miller – Product Security Officer, InFlyt Experience, Thales

Martin Strohmeier – Systems Security Researcher at the Department of Computer Science, University of Oxford

Paul Theron PhD – Co-Director of the Cyb'Air Research Chair, and Information Technologies Security Manager, Communications and Security, Thales

Jeffrey Troy – Executive Director, Aviation Information Sharing and Analysis Center

Raheel Qureshi – Chief Information Security Officer, North America, Thales

Matthew Vaughan – Director of Aviation Security (Airport, Passenger, Cargo, and Security Division), IATA

Beau Woods – Senior Fellow, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security, Atlantic Council

The objective of this report was to explore a considerably complex topic, which was discussed in both on- and off-the-record formats. Omissions of content or errors contained within the report are our own responsibility and not a reflection of the contributors whose candor and time has helped make this paper what it is.

Abbreviations

3D – 3-Dimensional

AAIB – Air Accidents Investigation Branch

ACARS – Aircraft Communication Addressing and Reporting System

ACAS-X – Airborne Collision Avoidance System X

ADS-B – Automatic Dependent Surveillance – Broadcast

AHM – Aircraft Health Monitoring

A-ISAC – Aviation Information Sharing and Analysis Center

ALARP – As Low As Reasonably Practicable

AM – Additive Manufacturing

APT – Advanced Persistent Threat

ASISP – Aircraft Systems Information Security/ Protection

ATC – Air Traffic Control

ATM – Air Traffic Management

CERT – Community Emergency Response Team

CNS – Communications, Navigation, and Surveillance

CPDLC – Controller-Pilot Data Link Communications

Data Comm – Data Communications

DHS – Department of Homeland Security

EASA – European Aviation Safety Agency

EFB – Electronic Flight Bag

FAA – Federal Aviation Administration

FANS – Future Air Navigation System

FMS – Flight Management System

GAO – Government Accountability Office

GCU – Generator Control Unit

GNSS – Global Navigation Satellite System

GPS – Global Positioning System

GSM – Global System for Mobile Communication

IATA – International Air Transport Association

ICAO – International Civil Aviation Organization

IFE – In-Flight Entertainment

IoC – Indicators of Compromise

IoT – Internet of Things

IP – Internet Protocol

IPv6 – Internet Protocol Version 6

ISAC – Information Sharing and Analysis Center

IT – Information Technology

MLAT – Multilateration

NextGen – Next Generation Air Transportation System

NIS – Networks and Information Systems

NTSB – National Transportation Safety Board

OEM – Original Equipment Manufacturer

OIG – Office of Inspector General

PBN – Performance-Based Navigation

PNT – Positioning Navigation and Timing

RF – Radio Frequency

RTS – Remote Tower Service

SA – Situational Awareness

Sat Comm – Satellite Communications

SDR – Software-Defined Radio

SESAR – Single European Sky ATM Research

SMS – Safety Management System

SOC – Security Operations Center

STIP – Security Technology Integrated Program

SWIM – System Wide Information Management

TCAS – Traffic Collision Avoidance System

TCP – Transmission Control Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TSA – Transportation Security Administration

UAS – Unmanned Aircraft System

VHF – Very High Frequency

Preface

This is a boom time for the aviation industry. The ten-year average for passenger growth hovers around 5.5 percent globally, aviation accidents and incidents are down to their lowest levels, profits are up due to historically low oil prices, and increasing use of technology is transforming efficiency and passenger experience.[3] Yet this study indicates that the aviation industry is likely to experience cybersecurity challenges similar to other industries that have embraced the 'digital revolution.' History is replete with examples of 'secure' systems from all sectors being critically compromised by adversaries in some form. As the aviation industry moves forward, its focus must be on both understanding and managing cyber risk and developing cyber resilience.

History is replete with examples of 'secure' systems from all sectors being critically compromised by adversaries in some form.

The primary objective for the aviation industry is to operate safely in what is a challenging environment. Accidents or incidents tend to be high profile and can severely impact stakeholder and consumer confidence. Efforts to improve aviation safety and security have been highly successful despite significant risks and advanced threat actors, and the industry is presently thought to be as safe as it has ever been. As a result, the industry is thriving; however, such growth is also becoming the driving force behind a number of challenges that the aviation industry now faces.

An increasingly connected and 'always on' population is leading to demands for evermore technologically advanced services and connectivity even while airborne. This evolution is not just driven by business requirements but also by competition to offer always improving in-flight entertainment and connectivity. As such, access to the Internet onboard passenger aircraft is now increasingly seen as the norm rather than the exception, and demand for bandwidth is on the rise.

Additionally, where the aviation industry can engage with passengers is changing. What was previously 'takeoff to landing,' is now evolving to 'gate to gate' and 'booking to baggage.' This is giving the airline industry more opportunity to offer seamless and enhanced passenger services that are not only attractive to passengers but attract more revenue. The diversity of digitization opportunities is driving airports and service providers to increasingly interoperate and improve efficiency, striving to safely and securely manage higher passenger numbers at the same time as offering additional passenger services.

But it is not just passengers that are demanding connectivity. As airliners become evermore complex, with pressures to maintain efficiency and serviceability, many airlines and aircraft manufacturers are connecting aircraft systems to ground services. This permits live monitoring of aircraft systems to quickly highlight engineering or servicing issues while airborne and facilitates considerably quicker resolutions. Shortening the time taken to maintain or resolve aircraft issues can result in large efficiencies across the entire fleet and considerable savings.

Finally, digitization and innovation go hand in hand as airlines and aircraft manufacturers seek greater efficiency and specialization across service providers and along a complex supply chain. Increased levels of interaction between disparate suppliers is seen as critical to reducing time to market and maintaining standards. But the challenges of securing such a critical supply chain are considerable as the industry attempts to seize opportunities such as the rapid growth in 3-dimensional printing technology and novel materials.

Globally, airspace is starting to reach a saturation point as more aircraft are squeezed into finite airspace managed by many legacy systems. There are a number of initiatives to increase efficiency through procedural measures, but increasing digitization of Air Traffic Management (ATM) is seen as the cornerstone of generating spare

3 "Another Strong Year for Air Travel Demand in 2016," IATA, press release, February 2, 2017, http://www.iata.org/pressroom/pr/Pages/2017-02-02-01.aspx.

Photo credit: Richard/Flickr.

capacity. This transformational project, being replicated around the globe, will see the rollout of digital, interconnected systems that permit greater airspace flexibility and higher traffic densities.

While the aviation industry's move toward digital connectivity is understandable, the challenge lies in the fact that the systems involved are critical to delivering safe operations involving human life. Previously, aviation systems were relatively secure due to the bespoke nature of their design, isolation from other systems, and little in the way of communication protocols, but aircraft are no longer 'air-gapped.' ATM is no longer isolated and ground services and supply chains are gradually becoming fully integrated into an interconnected digital world. In such a world, vulnerabilities will be found where they were not anticipated, adversaries will attack that which was not predicted, and systems which 'cannot fail'—can fail.

Balancing opportunities and risk in this digital revolution will be key. In aerodynamics, when an aircraft is going fast at high altitude, it can place itself in an aerodynamic 'conundrum.' Slowing down can cause a 'stall,' the loss of lift over the wings, but going faster can cause a loss of control. In this 'coffin corner,' the margins of too fast or too slow can be small, and requires a fine balance and delicate handling. The digitally connected aviation industry faces a similar conundrum requiring a fine balance. Too much regulation and restriction on innovation may stifle growth, but too little consideration of potential risk may leave critical services exposed to adversaries. Achieving the right balance will take considerable collaborative effort from all aviation stakeholders.

Aim of the Report

This report takes a broad look across the aviation cybersecurity landscape to better understand the risks and subsequent actions that may be taken to maintain stakeholder trust. It has become very clear from the research that a technologically advanced, connected aviation industry faces issues that are systemic in nature and global in scale. Focusing on technological failings may overlook issues with foundations, strategies, governance, and risk decisions made months or years prior. This report aims to promote a top-down vision of where aviation is, where it needs to go, and how it might get there. It does this in four ways:

1 – Catalyzes a dialogue about aviation cybersecurity and safety that preserves trust in the sector

This report is meant to increase dialogue across all stakeholders in the aviation sector by highlighting what is and can be done about cybersecurity and cyber safety issues. Generating such dialogue is critical to generating shared understanding and collaboration globally and across multiple stakeholder groups. No one perspective has all the solutions to the complex, safety critical challenges. Increasing dialogue across the aviation industry, cybersecurity industry, and policymakers brings opportunity for shared perspectives and solutions.

2 – Proposes methodologies to preserve trust in the aviation ecosystem

Aviation safety is enshrined across the entire aviation ecosystem—whether through people and culture, process, or technology—it is well governed, well understood, mature, and effective. This has fostered high levels of trust across customers, staff, shareholders, and a diverse set of stakeholders. But now, with cyber threats arrayed against the increasingly complex, networked technologies underpinning aviation safety, it is necessary not only to reevaluate the nature of this trust, but preserve it, recognize when it is being lost, and design the ability to quickly recover it.

3 – Proposes foundations for aviation cybersecurity

This report will approach the challenge of improving aviation cybersecurity by viewing it as a global system of systems that functions within small but well-defined safety margins with human operators at its core. A broad analysis of the cyber challenges facing the aviation ecosystem will lead to the development of a foundational understanding. This understanding will then be used to explore how the aviation ecosystem should be coalescing and moving forward to best respond to the challenges it faces.

4 – Proposes innovative aviation cybersecurity ideas and strategies for all stakeholders

The challenges are not just technical—they extend across perceptions, processes, governance, and cultures. This report's aim is not simply to highlight such challenges, but also to suggest how all stakeholders might maximize the benefits of their relationship, demonstrate ways in which they can productively work together, and communicate how policies and strategies need to develop in order to support such relationships.

Scoping and Focusing the Problem

The report will examine aviation aspects of both cybersecurity and cyber safety. It is clear that cyber safety, captured in this report as preventing adversarially instigated physical harm, must be the priority. But harm can be more than physical. For the aviation industry to be globally prosperous, it must also focus on appropriate cybersecurity to protect what it values, be it tangible or intangible.

As captured in the report, the stakeholders of the aviation industry directly enable the global movement of people and cargo via air: from the building of aircraft/unmanned aircraft systems to flight itself. But such a definition risks excluding the multitude of key additional aviation stakeholders such as governments, international organizations and associations, cybersecurity researchers, passengers, etc. Therefore, when discussing all of these stakeholders they will be referred to as the aviation ecosystem. Although helicopters are not specifically discussed within the report, their cybersecurity challenges are very similar to their fixed-wing counterparts. Similarly, the burgeoning commercial space industry is not specifically included in this report and, though it can be assumed that many of the cyber challenges and solutions may be similar, it merits further research. This would create a holistic view of the cybersecurity challenges facing aerospace as a whole.

When attempting to scope and focus the challenges facing a connected aviation industry, cyberattacks are highly likely to impact more than just aviation. Aviation is a cornerstone of national and international commerce, trade, and tourism, which means even an isolated incident could spark a wider crisis of confidence in the entire sector. The potential impacts on stock market value, stability, and national gross domestic product make securing and protecting the connected aviation world a critical element of national security. These effects must be considered as much as the aviation industry's components, systems, and companies when assessing cyber risk. This brings a shared responsibility upon all industry stakeholders to reduce the likelihood of a single 'weak link' impacting the entire commercial, national, and international ecosystem.

This principle of shared risk is not new. It has been woven into how physical security is managed across the aviation ecosystem for many years, and it continues to help frame the scope and nature of the challenge. Accordingly, this report adopts the same perspective of shared responsibility across all stakeholders and explores all aspects of people, processes, and technologies that will underpin a

safe and successful global aviation industry into the future.

A priority for all stakeholders within the aviation industry is to continually drive risk of accident, incident, injury, or loss of life down 'As Low As Reasonably Practicable' (ALARP). As safety systems utilize complex technologies, the ability to maintain ALARP in the face of adversarial motivations will arguably need careful understanding and management. This report will focus on the challenge of maintaining cyber safety and the wider context of how cybersecurity plays a critical role in maintaining broader trust and positive stakeholder perspectives.

Unlike commercial air operators, military air operators must assume that at some point they will be operating in a hostile environment where an advanced adversary is targeting them to deny, degrade, or disrupt their operations. One might contend that commercial aircraft face less of a threat. But, as history has shown, cyber adversaries care little about the nature of the target or the route to affect it. With many military air forces around the world now militarizing commercial aircraft, their vulnerabilities may be the same. Thus, this report will examine whether the military approach to such challenges holds lessons for the commercial industry and whether there is potential value in collaboration.

When looking across the aviation ecosystem—the totality of its activity and what it supports—its value is undeniable. But to realize and protect that value takes a global, complex, highly interdependent system of systems managed by passionate personnel. This report looks at this ecosystem's intertwinement with connected technologies, and how it may maintain safety and security in the face of adversary intent.

The Aviation Landscape

Section Takeaways

- 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.

The aviation industry has, on the whole, been enjoying a period of strong growth since recovering from the 9/11 attacks. This growth in the strength of the market has also been matched by the increasing diversity and sophistication of passenger services and increased use of technology.

Aviation operates within a naturally hazardous environment; that it has statistically become one of the safest modes of transportation is a credit to all who work within the industry. But the aviation industry is en route to becoming fully digital, with connected technologies linked to critical services. On this transition, it has an obligation to at least maintain or, where possible, improve the hard-won safety record that it currently enjoys. Doing this while balancing novel risk and potential opportunity in a commercially competitive environment will be challenging. It will require industry, policymaker, and other stakeholder collaboration to build on known effective practices, and innovate new ones where needed. Understanding their values and motivations may help identify the drivers to improve cybersecurity efforts.

Values and Motivations

With 60 percent growth over the last ten years, and in spite of such events as 9/11 and the financial crisis, the aviation industry appears to be "resilient to external shocks."[4] The last three years have seen the best global net profits in the history of the industry and the profit forecast for 2017 hovers around $30 billion.[5] Profits, mainly driven by greater efficiencies and low oil prices, are not the only numbers in the global aviation industry to see growth. As a result of expansion and increased demand, numbers have reached around 4 billion passengers and 55.7 million tons of cargo a year.[6] The International Air Traffic Association (IATA) expects passenger growth to nearly double in the future, reaching 7.2 billion passengers by 2035.[7] There is an increasing demand for new aircraft to support this growth. Boeing forecast that over 41,000 new aircraft with a value of $6.1 trillion will be required over the next twenty years, an increase of 3.6 percent on their previous forecasts.[8] But focusing exclusively on the aviation industry belies the value it adds to other sectors and wider gross domestic product (GDP).

---

4 *Growing Horizons*, Airbus, 2017, http://www.airbus.com/content/dam/corporate-topics/publications/backgrounders/Airbus_Global_Market_Forecast_2017-2036_Growing_Horizons_full_book.pdf.

5 "Another Strong Year for Airline Profits in 2017," IATA, press release, December 8, 2016, http://www.iata.org/pressroom/pr/Pages/2016-12-08-01.aspx.

6 Ibid.

7 "IATA Forecasts Passenger Demand to Double Over 20 Years," IATA, press release, October 18, 2016, http://www.iata.org/pressroom/pr/Pages/2016-10-18-02.aspx.

8 "Boeing Raises Forecast for New Airplane Demand," Boeing, press release, June 20, 2017, http://boeing.mediaroom.com/2017-06-20-Boeing-Raises-Forecast-for-New-Airplane-Demand.

Incheon International Airport on the outskirts of Seoul, South Korea. *Photo credit:* Ken Eckert/Wikimedia.

According to 2014 figures, although the global aviation industry directly supports around 9.9 million jobs, there are another 16.4 million jobs that are either indirectly supported or generated by the industry; these are in addition to the 36.3 million that make up the tourism industry. This translates to $2.7 trillion of economic impact and 3.5 percent of global GDP.[9]

As much as the industry is profitable, the margin for error remains small, and incidents that negatively impact finances or investor confidence can have considerable effect.

When British Airways suffered an IT failure, caused by the misoperation of an uninterruptable power supply, it resulted in 726 flight cancellations, seventy-five thousand stranded passengers, and total costs of around £80 million.[10]

Delta Airlines lost power at its operations center on August 16, 2017, which caused a five-hour outage. As a result, around two thousand flights were cancelled at a cost of $150 million.[11]

Although these were accidental outages and not the product of malicious activity, they demonstrate how quickly even simple failures can rapidly snowball, destabilize operations, and impose considerable costs. The more that adversaries observe how the failure of one system may scale and cascade in a connected industry, the greater their motivations will be to explore the 'art of the possible.' This risk should be a key motivator for the aviation industry to not just improve cybersecurity but to collaborate across systems.

Clarifying, refining, and increasing the motivations for the aviation industry to improve cybersecurity is key to mitigating future risk. Some elements of the aviation and cybersecurity sectors have made good progress in developing cybersecurity methodologies and capabilities, but this is not the case across the entire industry.

9 *Aviation Benefits Beyond Borders*, IATA, July 2016, https://aviationbenefits.org/media/149668/abbb2016_full_a4_web.pdf.

10 Tobias Buck and Peggy Hollinger, "BA Faces £80m Cost for IT Failure That Stranded 75,000 Passengers," *Financial Times*, June 15, 2017, https://www.ft.com/content/98367932-51c8-11e7-a1f2-db19572361bb.

11 Chris Isidore, "Delta: 5-Hour Computer Outage Cost Us $150 Million," CNN Tech, September 7, 2016, http://money.cnn.com/2016/09/07/technology/delta-computer-outage-cost/index.html.

Encouraging and motivating the entire aviation industry to see value in cybersecurity improvement is as challenging as it is essential. Regulatory compliance may help, but as other industries have discovered, even the most highly regulated industries will suffer breaches, and being compliance-centric (as opposed to adversary-centric) has limitations. The inclusion of cybersecurity requirements within many insurance policies may help, but they are not the only potential motivators.

The speed of innovation, technological advancement, and adversary capability is potentially outstripping policy and regulatory development in many areas of the aviation ecosystem.

Financial investors who, so far, have remained relatively quiet in this matter, could be a stakeholder group with considerable ability to motivate. As the International Civil Aviation Organization (ICAO) and other bodies increasingly emphasize required improvements in cybersecurity, investors may become even more focused on the cybersecurity of their investment. This will not only require an understanding of aviation cybersecurity risk but also the burgeoning attempts to use regulation and policy to manage it.

Research shows that, although there is growing industry awareness of the need to improve cybersecurity, companies may be hesitant to roll out, buy, or upgrade cybersecurity capabilities. The proffered reason for this hesitancy was that, although standards may be in draft, national and international bodies have yet to set aviation cybersecurity regulations and interoperability standards. Waiting was seen as preferable to selecting a methodology or technology that may soon become incompatible or cannot interoperate with the declared 'industry standard.'

But such a waiting game does not just hold back the aviation industry, it also holds back the creation of a strong and diverse cybersecurity industry that supports the aviation industry. In order to move forward, there must be clear and unambiguous policy direction on interoperability standards from international and national bodies.

Aviation Cybersecurity Policy

The speed of innovation, technological advancement, and adversary capability is potentially outstripping policy and regulatory development in many areas of the aviation ecosystem. Coalescing and rapidly maturing national and international policy will be critical to get ahead of the technology and the risks.

There are a great number of global and national bodies involved in the aviation industry, and many of them are progressively contemplating the cybersecurity challenge. Since aviation is a global industry, the ICAO, under the auspices of the UN, has the responsibility of setting international aviation standards and acts as a channel for nations to discuss all aspects of the trade. This role of leading and enabling a structural framework for dialogue and standardization is critical to securing and promoting a global industry. It is a model that has worked well for many years, but due to the nature of such large international bodies, negotiation and agreement may be a slow evolution.

But this evolution is happening. In 2016, the 39th session of the ICAO assembly adopted a resolution to address cybersecurity in civil aviation.[12] This highlighted the danger posed by rapidly evolving malicious threat actors and the urgent need to counter them through collaborative industry efforts. The ICAO called upon member states to collaborate in the development of an ICAO cybersecurity framework, which hopefully will bring structure to the challenge. The resolution was reinforced by the declaration that took place at the ICAO cybersecurity conference in Dubai in 2017 calling for states to mitigate cyber risk and develop legislative frameworks to take action against "actors of cyber-attacks."[13] An additional deterrent element was incorporated that declared "cyber-attacks against civil aviation must be considered an offense."[14] This focus on not just cybersecurity but establishing norms of international behavior is a welcome development that adds depth to the dialogue nationally and internationally.

Although there are a number of national initiatives around the globe that aim to improve internal aviation cybersecurity policy, a key effort in the

12 "Assembly – 39th Session: Resolutions Adopted by the Assembly," ICAO, October 2017, https://www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf.

13 "Declaration on Cybersecurity in Civil Aviation," ICAO Cyber Security Summit, April 4-6, 2017, https://www.icao.int/Meetings/CYBER2017/Documents/Final%20text%20Declaration%20(2).pdf.

14 Ibid.

United States is the 'Cybersecurity Standards for Aircraft to Improve Resilience Act of 2016,' or the 'Cyber Air Act,' proposed by Senator Edward Markey.[15] This Act creates a feedback loop of improving knowledge and visibility to update standards and regulations on "aircraft systems and maintenance and ground support systems for aircraft," with requirements to identify "electronic entry points" to aircraft so that they may be protected by actions like isolating critical systems from non-critical systems.[16] Concentrating on the aircraft is a good step in understanding a key element of the challenge; if the work goes forward, it will nest well with wider industry efforts.

The categorization of aviation as an element of critical national infrastructure is highlighted in both the United States and Europe. For example, the Networks and Information Systems (NIS) Directive in Europe covers the aviation sector. In the United States, aviation has increasingly been assimilated into the Department of Homeland Security (DHS) Authorization Act of 2017.[17] This Act recognizes the value in understanding the dangers, calling for future threat assessments to include a cyber component and a yearly threat assessment with a spotlight on risks to aviation transportation systems.

Section 561 contains a short segment specifically about aviation cybersecurity. This initially sets out that the Secretary of Homeland Security shall "not later than 120 days after the date of the enactment of this Act, develop and implement a cybersecurity risk assessment model for aviation security, consistent with the National Institute of Standards and Technology Framework for Improvement Critical Infrastructure Cybersecurity." If the Act is passed, developing and implementing such a risk assessment model within 120 days will be a challenging goal to accomplish, given the international landscape of aviation cybersecurity and its intersections between public and private stakeholders.

As the cybersecurity industry partners with the aviation industry, it must ensure that it supports and augments, not weakens what currently works well. For example, a large part of the Act is dedicated to the importance of cybersecurity information sharing, but does not yet consider how to incorporate this practice into the aviation safety information-sharing systems already in place. Parallel aviation safety and cyber safety/security systems may work, but at the risk of drastically increasing both the burden of management and complexity of governance.

The DHS Authorization Act of 2017 also considers that the "minimum security standards for airport security set forth by the Chicago Convention . . . are not robust enough in the current threat environment where we have repeatedly seen terrorist organizations planning attacks targeting aviation . . ." and directs the US representative to ICAO to "pursue improvements to airport security."[18] As this report will explore, the aviation industry faces not just a physical security threat but also a cybersecurity threat that touches every aspect of both safety and non-safety critical operations. Therefore, as the US representative to ICAO starts to "take a leadership role at the ICAO . . . to raise these standards," there is great opportunity to incorporate consideration of the growing cyber threat.[19]

There is growing interest in the subject of securing a modern aviation industry on the national and international stage. It is probable that the various initiatives will converge and evolve, easing the industry's efforts to make headway. Yet progress will be slow without a thorough understanding of the landscape, its stakeholders, and its challenges. The more these components are understood and managed, the greater the ability to achieve accuracy and efficiency.

15 Cyber AIR Act, S. 2764, 114th Cong. (2016), https://www.markey.senate.gov/imo/media/doc/Cyber AIR Act 4-7-16.pdf.

16 Ibid.

17 Department of Homeland Security Authorization Act of 2017, H.R. 198, 115th Cong. (2017), https://www.congress.gov/115/crpt/hrpt198/CRPT-115hrpt198.pdf.

18 Ibid.

19 Ibid.

Challenges Facing a Connected Aviation Industry

SECTION TAKEAWAYS

- The aviation industry has decades of experience in preventing safety and security issues, but the cybersecurity and cyber safety challenge is comparatively novel.
- It may take longer to develop and replace aviation systems than it does for adversaries to develop capabilities, creating a challenge to accurate risk assessments and threat models.
- Military aviation shares a number of cybersecurity challenges with commercial aviation but anticipates a more aggressive threat and manages risk accordingly.
- Adversary numbers, capabilities, and willingness are increasing, as is exposure and attack surface. Yet industry perceptions vary on the urgency and severity of the challenge.

> "Cyber attacks on the aviation sector have so far been low-level and caused limited impact, but the consequences of a successful malicious cyber-attack on civil aviation operations could potentially be catastrophic."[20]

The sentiment in the above quote was a common theme across the research for the report and many contributors shared the impression that the industry has "gotten away with it so far." Other major industries have already learned how difficult it can be to get cybersecurity right. A globally connected aviation industry is at risk of epidemiological failure modes, where failure in one location can quickly spread to the whole, outpacing approaches to response in isolated (or even enterprise IT) environments. Such risks are globally systemic with cascading failure modes to match.[21]

The aviation industry has a long history of minimizing the risk of accidental harm with well-established design principles, safety margins, and Safety Management Systems (SMS) that operate under meticulous procedures to promote safe operations, prevent accidents, and foster a proactive safety culture. The aviation industry also has considerable experience in preventing unlawful interference of operations by actors attempting to compromise security and do harm. Overall, for a complex, global operation the aviation industry has been successful in achieving safety and security, and demonstrating that their stakeholders can trust them. When incidents or security breaches

20 "Assembly – 39th Session: Agenda Item 36 Coordinating Cybersecurity Work," ICAO, working paper, September 20, 2016, https://www.icao.int/Meetings/a39/Documents/WP/wp_236_rev1_en.pdf.

21 Margareta Hanouz, *Understanding Systemic Cyber Risk, Global Agenda Council on Risk & Resilience*, World Economic Forum, white paper, October 2016, http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf.

do happen, the industry can easily demonstrate changes or improvements to safety and security procedures to recover trust. Recovering trust after a cybersecurity incident, however, may be considerably harder.

For an industry accustomed to demonstrating safety and security, the complexity of connected systems and the intricacies of defending them brings a challenge. In the event of a cybersecurity incident or an exposed vulnerability, the aviation industry must be able to demonstrate assurance and rebuild trust quickly. Because many cybersecurity mitigations are technical, it will be a challenge to demonstrate effectiveness to a non-technical audience; declarations of improvement after an incident may not be enough. This potential fragility and difficulty in rebuilding trust means that, as the industry seeks to develop resilient systems, it must also seek to develop a resilient trust with its key stakeholders.

Understanding the Threat, Knowing the Risk

History has shown that cyber adversaries and their capabilities evolve and adapt surprisingly quickly. This may be particularly challenging in the aviation industry where many of the systems considered the backbone of the industry have long development periods, where policies and design standards are fixed early, and updates take a considerable amount of time. In order for the aviation industry to accurately assess and predict risk, it is imperative to understand the current threats and their potential implications.

There are numerous examples of cyberattacks in which the victim organization had high confidence in its ability to defend itself against what it thought were its threats right up to the point that a compromise was discovered. This cycle is becoming so commonplace that it is no longer surprising.

When assessing risk, many sectors—including aviation—will characterize the sophistication of threat actors into groups such as: Advanced Persistent Threat (APT), organized criminal gang, hacktivist, etc. Many businesses, however, do not consider APT to be a threat in their risk assessments due to their own perception as a target. But as seen with numerous highly public breaches, early claims of APT actor involvement may be more in hope for absolution than fact because it could not have been 'foreseen' or countered.

There is an argument that over-reliance on threat actor characterization in risk assessment may undermine accuracy. After all, recent history increasingly demonstrates that technical ability, scale, or nature of compromise is no longer an indicator of threat actor. Well-resourced threat actors will use unsophisticated tools to both save money and misdirect attribution, unresourced individuals with key skills can develop sophisticated tools.

Some contributors considered that aviation industry threat models often underestimate adversary ability or the increasing sophistication of that ability. Getting the threat model correct is essential for understanding true risk levels. There should be cyber safety requirements for critical systems that could cause loss of life if compromised. For example, the risk of catastrophic failure for flight critical systems must be assessed as extremely improbable ($1x10^{-9}$) and validated by test and analysis. If the cyber threat model is underestimated it may give the incorrect impression that an acceptable level of risk has been achieved.

Notwithstanding the above, both the aviation and cybersecurity industries have experience with the threat of the malicious insider. The aviation industry has put much focus on attempting to mitigate insider threats, mainly to physical security. So too in cybersecurity, many of the high-level processes in spotting and preventing a trusted insider from abusing trust are the same. Methodologies such as employee screening, layered security measures, and looking for anomalous behavior will be common ground for both industries as they move forward in finding threats.

Correctly assessing risk is as critical as it is difficult with threat actor ambiguity, risk complexity, and landscape variability. Defending in the face of ambiguity and complexity can be done, but it will take additional effort in preparing for a determined adversary, and efforts to better understand and reduce the attack surface of systems that could be affected. The following two sections explore this.

Becoming a Bigger Target

The aviation industry has long been a target for malicious actors. As it increasingly connects services and systems, its potential attack surface of systems that an adversary could interfere with is growing considerably larger and more complex.

Increasing technology and connectivity has brought new opportunities for malicious actors to target the aviation industry. On the ground, this ranges from juvenile actions like disrupting airport operations to state sponsored activity such as the disruption of airport video screens and audio announcements for the dispersion of propaganda.[22] In the air,

22 Paul Festa, "DOJ Charges Youth in Hack Attacks," CNET, March 18, 1998, https://www.cnet.com/news/doj-charges-youth-

Photo credit: Capa Pictures/Thales.

multiple researchers have claimed credible attacks on both ATM systems and aircraft. Terrorist groups such as 'The Tunisian Hackers Team' have already threatened to use cyberattacks on the aviation sector: ". . . next time, there will be an attack on your airness [sic]. We will work on gaining control of your airports' computers—and you know very well that we can do this—and of the electronic sector."[23]

With a rapidly expanding, multi-stakeholder owned attack surface, vulnerabilities will exist in all systems—it is only a matter of when they are discovered and by whom. Adversaries are always seeking to understand the 'art of the possible' and the benefits they can reap from it. Attacks against the aviation industry have so far had comparatively little impact, which may lead to a feeling of imperviousness. But, as other industries will attest, such perceptions rarely last.

Perceptions of the Threat

How a cyber threat is perceived will be critical in understanding risk and managing it. When researching for this report, it became apparent that the wide variety of perceptions may be one of the biggest challenges that the aviation industry faces.

One off-the-record contributor was particularly blunt about some perspectives in the aviation industry: "It's going to take the factory over the road burning down before they buy a sprinkler system." Others offered anecdotes of how concern about potential aviation vulnerabilities had been

in-hack-attacks/; Brett Davis, "Hacking Attack At Vietnam Airports Another Chapter In South China Sea Dispute," *Forbes*, August 13, 2016, https://www.forbes.com/sites/davisbrett/2016/08/13/hacking-attack-at-vietnam-airports-another-chapter-in-south-china-sea-dispute/#4dfd9be76e35.

23 Anthony Kimery, "Tunisian Hackers Announce Cyber Jihad Against US Banks, Airport Computer Systems," *Homeland Security Today*, July 4, 2014, http://www.hstoday.us/briefings/daily-news-analysis/single-article/exclusive-tunisian-hackers-announce-cyber-jihad-against-us-banks-airport-computer-systems/7c3d2373e69fa9319e521816ce539b7d.html.

dismissed out of hand because such a vulnerability was impossible.

Although there are many in the aviation industry that perceive and understand the complex nature of the cybersecurity challenge, it is necessary that everyone in the industry attains the same level of perception and understanding. This is key to preventing the dismissal of potential risk and to promoting collaborative dialogue that values multiple perspectives.

The aviation industry already acknowledges and manages the risk of failure: the majority of aviation systems are built to fail predictably in a manner that does not compromise safety. As the industry increases its attack surface and becomes a more enticing target for cyber adversaries, there is a risk of creating considerable unpredictability. Dealing with this unpredictability will require different stakeholders with varied perceptions working together. Closing the gap between these perceptions will bring many of these challenges into clearer focus and better allow the industry to see risk and opportunity. Many of these considerations are brought to the fore in the next section, which explores the challenges of the connected aircraft.

THE MILITARY PERSPECTIVES OF AVIATION CYBERSECURITY

As military aircraft increasingly become as connected as their civilian counterparts, how the military perceives and approaches the challenge of securing aircraft and systems within environments that face physical, Radio Frequency (RF), and cyber threats may have lessons for the commercial aviation industry.

Military assessment of adversary threat, capability, and risk may often be based on classified assessment of threat actor capability and an anticipation of aggressive intent and determination. This means that military threat models will be considerably more robust than their civilian counterparts. Such a robust threat model is leading to an increasing amount of testing and assurance of aircraft and systems.

As an example, the KC-46A aerial refueling aircraft, based on the civilian Boeing 767-200ER, is the first increment of replacement tankers for the United States Air Force. The aircraft has gone through a considerable modification program to increase its survivability in high threat environments. This has included a cyber threat assessment with a comprehensive vulnerability and penetration testing program, ranging from individual systems up to live aircraft.[1]

These considerations and other efforts appear to set the bar for military aviation cybersecurity considerably higher than their commercial counterparts. This seemingly makes sense since commercial entities will not be involved in targeted military operations. However, the circumstances are complicated by the fact that many air forces seek to save costs by modifying commercial aircraft and systems for use in military operations. This means that adversaries will assess these aircraft and systems to find vulnerabilities, which may be present on both the military and civilian versions. In addition, recent history has shown that cyber adversaries will target anything to achieve their aims, which may skew the commercial threat model. As the military tests its systems and finds vulnerabilities, however, there is opportunity for the wider industry to gain.

For example, during the testing of the KC-46A, vulnerabilities were discovered not just in the aircraft but also in the "government furnished equipment."[2] The military may have found those vulnerabilities, but there is arguably a critical requirement to patch both the military and commercial fleets. Although the sharing of vulnerability knowledge between government and industry is a debated topic, it is hoped that the processes are in place to rapidly enable such sharing with the aviation industry.

A connected system, commercial or military, brings the potential for adversaries to connect and disrupt. The strengthened security of military aircraft and systems may motivate threat actors to target commercial systems due to their perceived comparative weakness. Therefore, the commercial industry may have to both learn from and act on military approaches to cybersecurity."

1 "FY15 Air Force Programs: KC-46A," DOT&E OSD, 2015, http://www.dote.osd.mil/pub/reports/FY2015/pdf/af/2015kc-46a.pdf.

2 Ibid.

The Connected Aircraft

SECTION TAKEAWAYS

- 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.
- The diversity, complexity, and responsiveness of global supply chains is at odds with the agility needed to address cybersecurity risks across the design and manufacturing processes.
- While new and emerging capabilities like Additive Manufacturing (AM) and UAS are transforming the aviation sector, they also present novel cybersecurity risks that are not yet fully understood.
- 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.
- Aircraft now contain complex data networks, yet the ability to monitor them arguably lags behind comparably complex ground-based networks, as does the ability to avoid and respond to potential cybersecurity incidents.
- Rates of change in technology appear to be faster than governance development, so practices will move faster than standards and regulations; yet some form of rigor, accountability, and assurance is necessary to preserve trust in the sector.

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.

Since the laws of aerodynamics remain unchanged, the evolution of aircraft design has always had steady, visible progress. Yet when it comes to aircraft technology, saying there is a generational difference is an understatement.

The concept of air travel is being constantly redefined. Not long ago, an airliner delivered luxurious service in isolation from the rest of the world. Now, as the aviation industry responds to customer demand, having seamlessly connected services throughout the flight is considered essential. This transformation is not just in passenger services. As greater efficiency is sought, connected technology increasingly transforms how aircraft are serviced and operated. These aircraft are not just connected to airline or air traffic services, but also to the wider Internet, facilitated by both satellite and ground stations. The days of asserting that aircraft are 'secure' by means of isolation are over. There is now a clear requirement to secure and assure connected aircraft. As already discussed, it is not enough to say an aircraft is safe and secure; to maintain stakeholder and passenger trust, it must be possible to demonstrate it.

In the early days of aviation, demonstrating safety and security was simple. An aircraft would be designed, tested, and built at the same location. Now, tiers of global suppliers come together to produce one aircraft. Where aircraft structures and components were once hand-shaped from wood and aluminum, composite materials and 3-Dimensional (3D) printing are now increasingly standard. Where 'fly-by-wire' literally meant piano wire in a physical link from the pilot's hand to the control surface, a computer is more likely to make decisions based on thousands of parameters in addition to crew input. Pilots are now digitally abstracted from the platform they are flying. They

tell the computer what they want the aircraft to do, and the computer then assesses it before making it happen. In the event of computer failure, backup computers are available so that the systems 'fail-safe' in a manner that permits the aircraft to land.

Aircraft are now digitized and contain millions of lines of code; writing, verifying, and securing it is an increasingly difficult and complex task. The challenge of that task is not just measured in the rate of code production, but also in its maintenance and security across the aircraft's lifecycle. Many industries have discovered that the ability to quickly identify and patch software vulnerabilities is a key requirement, but, according to one interviewee, modifying one line of safety critical software onboard an aircraft is currently estimated to take a year and cost around $1 million. There is a critical requirement to quickly deploy security updates, but the current time gap between vulnerability identification and remediation is a key concern. With regulators fully prepared to ground entire aircraft types until critical vulnerabilities are resolved, securely designing, manufacturing, and updating aircraft will be a critical part of the endeavor.

Manufacturing

The diversity, complexity, and responsiveness of global supply chains is at odds with the agility needed to address cybersecurity risks across the design and manufacturing processes.

With the backlog of orders for Airbus and Boeing hitting over 13,000 aircraft, equivalent to just under ten years at current manufacturing rates, the considerable efforts to speed up aircraft manufacturing is understandable.[24] Manufacturers are seeking to broaden their supply base by subcontracting and outsourcing production internationally in a drive to reduce costs and speed up aircraft delivery, or to secure regional financial incentives. This sometimes means each aircraft has different groups of suppliers located in different regions, but set standards on which they are expected to be delivered. The risk of such an extended supply chain is that the "manufacturer can never exceed the capabilities of the least proficient of the suppliers"—an argument that is applicable to both part delivery and cybersecurity.[25]

The wealth of intellectual property and proprietary data spread across the supply chain is considerable. Additionally, depending on the nature of that supply chain, some of that data may be liable to restrictions under the US International Traffic in Arms Regulations regime. Appropriately securing such data is a considerable challenge for the overall risk owner, having to balance trust, assurance, and risk with all their supply partners.

The additional and arguably more critical risk is that—through accident or design—a vulnerability could be created in either the part or the system being delivered. Such a potential vulnerability has weighed on the mind of contributors to the report, one of whom pointed out the challenge of finding such a vulnerability if it had been designed to not occur "until after 2000 cycles." In the face of such a risk, the only effective mitigation may prove to be resilient systems and the effort to assure and oversee.

Aircraft Systems

In a remarkably short period, aircraft systems have evolved from having minimal connectivity to having systems that are easier to discuss in terms of what is not connected. While this connectivity benefits the fuel economy, Aircraft Health Monitoring (AHM), and passenger experience, it arguably also increases exposure to onboard systems. Corporate IT security processes may fail to achieve the reliability and response times necessary for safe aviation.

This change in system design is driven not just by the growth of subtle insights and increased efficiencies provided by operational technology, but also by plans to transform the cockpit into a data-rich environment that supports the flight crew with previously inaccessible information. Passengers now enjoy a level of connectivity indistinguishable from their home or office environment.

Modern connected aircraft have seen a rapid growth in the amount of data they produce. It is estimated that by 2026, the global growth in aircraft-generated data could reach 98 million terabytes.[26] Much of this data is where evidence of adversary activity or intent will be visible. Being able to see into this data, protect it, and quickly analyze it for weak signs of compromise will be essential. Regulators are attempting to set

24 *Global Commercial Aerospace Industry: Aircraft Order Backlog Analysis*, Deloitte, July 2016, https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/ConsumerIndustrialProducts/ie-manufacturing-aircraft-order-backlog-analysis.pdf.

25 Dr. L. J. Hart-Smith, *Out-Sourced Profits – The Cornerstone of Successful Subcontracting*, Boeing, February 14-15, 2001, http://seattletimes.nwsource.com/ABPub/2011/02/04/2014130646.pdf.

26 Tim Hoyland, Chris Spafford, and Andrew Medland, "MRO Big Data – A Lion or a Lamb? Innovation and Adoption in Aviation MRO," Oliver Wyman, 2016, http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2016/apr/NYC-MKT9202-001MRO-Survey-2016_web.pdf.

Aircraft Communications

Satellite Communications

External signal, such as ADS-B

GSM In-Airplane Communications (data network)

Receiver and transmitter to external signals, such as ADS-B

Air Traffic Management Communications


Internet
GPS
Ground Receiver for Satellite
(aircraft - sat - Internet)
Data Center

Airbus plant in Toulouse, France. *Photo credit:* Lomita/Wikimedia.

standards that are practical, effective, and able to stand the test of time for these aircraft systems and the data produced.

Network Design

Aircraft designers are now expected not just to design the most aerodynamic exteriors, the most efficient engines, and the best passenger experience, but also to incorporate and exploit considerable computing power across the whole platform. This has resulted in aircraft networks evolving from simple, low bandwidth, point-to-point transfer of information to high bandwidth Transmission Control Protocol/Internet Protocol (TCP/IP) networks permitting considerably freer data flow than previously thought possible. Aircraft, like most other networks, are now a world of Wi-Fi routers, firewalls, and multi-core processors.

Such networks are split into several aircraft data domains according to how much trust and assurance is required:

- The aircraft control domain is comprised of systems and networks whose primary function is to support the safe operation of the aircraft.
- The airline information services domain contains systems and networks that provide non-critical aircraft services and support inter-domain connectivity.
- The Passenger Information and Entertainment Systems Domain (PIESD) provides and supports all passenger services such as entertainment, Internet connectivity, etc.

Although these domains have become standard terminology across the industry and appear simple, the underlying complexity may not be. When they were used by Boeing for their 787, the Federal Aviation Administration (FAA) considered it a ". . . novel or unusual design feature . . ." that was not covered by airworthiness regulations at the time.[27] The FAA requested that Boeing demonstrate the

27 "Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Isolation or Protection From Unauthorized Passenger Domain Systems Access," FAA, February 1, 2008, https://www.federalregister.gov/documents/2008/01/02/E7-25467/special-conditions-boeing-model-787-8-airplane-systems-and-data-networks-security-isolation-or.

safety and security measures put in place, only clearing the aircraft to fly after they had done so.

The computing requirements to manage networks and aircraft systems are increasing as they become more complex. At the same time, technological obsolescence makes it difficult to potentially expand or maintain services. It is understandable, therefore, that the industry is currently exploring the potential opportunities and risks of using multi-core processors; as chips become more complex, securing them becomes increasingly challenging.[28] Hidden services, or back doors, such as the one discovered by Skorobogatov and Woods in an Actel ProASIC3 chip, are difficult to find, and

28 Xavier Jean, Marc Gatti, Guy Berthon, and Marc Fumey, "MULCORS – Use of MULticore proCessORs in Airborne Systems," EASA, June 2011, https://www.easa.europa.eu/system/files/dfu/CCC_12_006898-REV07 - MULCORS Final Report.pdf.

3-DIMENSIONAL PRINTING IN THE AVIATION INDUSTRY

AM, or 3D printing, is a key and rapidly growing area of the aviation industry supply chain that merits a deeper examination of cybersecurity challenges. Though it started as a niche capability, AM parts are now widely used on commercial aircraft (over one thousand on the Airbus A350) and the industry is still rapidly growing.[1] Apart from the obvious advantage of less waste, AM printed parts can be lighter and stronger than their deductive predecessors. Additive printers can now create products in both fine detail and at scale using a multitude of materials. Since it is digital, however, there is immediate potential for concern.

An adversary looking to compromise the IT architecture of the printing process may have a few options available:

- Deny – Disruption or deletion of firmware, software, or product designs
- Compromise – Compromise of intellectual property through the theft of product design files
- Sabotage – Undetected modification of the printing process with the intention to weaken the products being produced

Arguably, 'deny' is the most recognizable of the risks and is familiar to the industry irrespective of the system. A unique aspect of 'compromise' when it comes to AM is that once the design file has been stolen, the adversary does not need to tool up a production line or build mock-ups to reproduce it. They can just print it. This makes AM printing design files highly sought-after for adversaries and likely to become a next wave of industrial espionage. The risk of 'sabotage' may be an order of magnitude more difficult for the adversary to achieve, but the outcomes could have a greater impact.

There have been several research projects covering cybersecurity vulnerabilities in AM. In one project, researchers found that it was possible to compromise either the printer or the design in such a way that the product was weakened in a manner undetectable with standard quality control methodologies.[2] A different set of researchers demonstrated the ability to weaken a design by accelerating the fatigue life of a propeller so that it failed catastrophically after two minutes of use. Additionally, for this attack, the researchers were able to demonstrate an attack chain from an external threat into the printer, and also the ability to insert the exploit into a worm that could be given sets of constraints and instructions.[3]

The AM industry was worth $11 billion in 2015 and is forecast to reach $27 billion in 2019.[4] With increased growth and uptake of AM in more and more critical areas, the risk of cyber adversaries seeking their own slice of value or disruption also grows.

1 Carrie Wyman, "Stratasys Additive Manufacturing Chosen by Airbus to Produce 3D Printed Flight Parts for its A350 XWB Aircraft," *Stratasys*, May 6, 2015, http://blog.stratasys.com/2015/05/06/airbus-3d-printing/.

2 Steven Eric Zeltmann, et al., "Manufacturing and Security Challenges in 3D Printing," *Journal of the Minerals, Metals, and Materials Society* 68, no. 7 (2016): 1872–1881, https://doi.org/10.1007/s11837-016-1937-7.

3 Sofia Belikovetsky, et al., "dr0wned – Cyber-Physical Attack with Additive Manufacturing," *CoRR*, September 1, 2016, http://arxiv.org/abs/1609.00133.

4 "3D Printing Comes of Age in US Industrial Manufacturing," PWC, April 2016, http://www.pwc.com/us/en/industrial-products/publications/assets/pwc-next-manufacturing-3d-printing-comes-of-age.pdf.

Photo credit: William Perugini.

once installed may prove difficult to mitigate if discovered after installation.[29]

Such challenges in system complexity became a reality for the Boeing 787. Not only did it use the Actel ProASIC3 chip, but the Generator Control Units (GCU) were found to have a software overflow that would cause them to go into fail-safe mode after being powered up for 248 days.[30] If the four GCU's had been powered up at the same time, they would stop producing power after 248 days "regardless of flight phase."[31] Boeing subsequently satisfied the FAA concerns, but it serves as an example of how difficult it is for the aviation industry and regulators to find issues in complex systems. Increased complexity is a given for the future of the industry. The ability to work through it, assure it, and regulate it will prove challenging. Adversaries will seek out where such complexity has led to oversight and potential system weakness. It will be crucial to find, fix, and collaborate on such weaknesses across the industry.

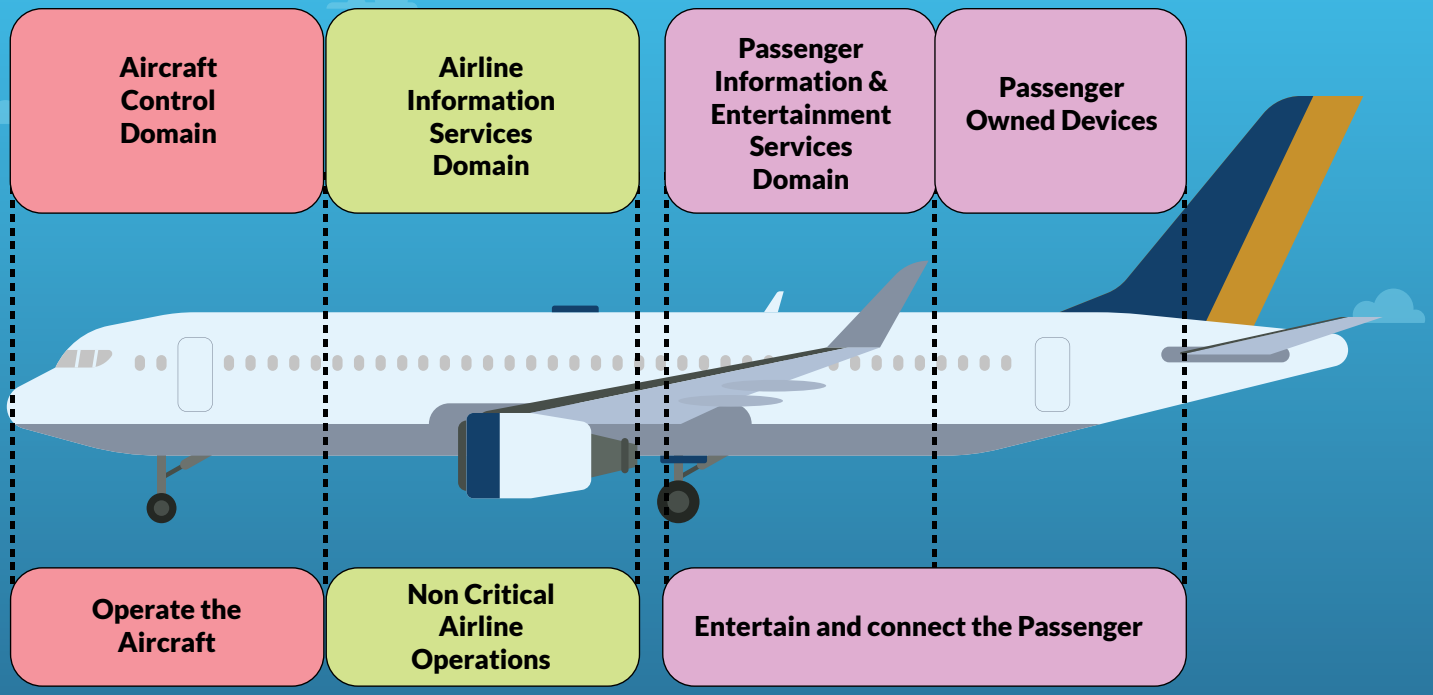
Much industry work has focused on building secure and trustworthy domains. But trust in complex systems can only be assured if it is possible to recognize when trust is being degraded and when components and systems can be entrusted to protect the whole. The ability to know when trust is compromised to take timely appropriate action is currently difficult, or almost impossible, on aircraft systems.

From discussions with contributors, this challenge is being explored and real time monitoring of aircraft systems may evolve to look much like any other terrestrial network. In the future, utilizing high bandwidth communications, aircraft network data may be transmitted back to a Security Operations Center (SOC) for monitoring and action much like a standard ground-based network. Some are actively

29 Sergei Skorobogatov and Christopher Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip," in *Cryptographic Hardware and Embedded Systems Workshop* (Leuven: International Association for Cryptologic Research, 2012), http://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf.

30 Charles Arthur, "Cyber-Attack Concerns Raised over Boeing 787 Chip's 'Back Door,'" *The Guardian*, May 29, 2012, https://www.theguardian.com/technology/2012/may/29/cyber-attack-concerns-boeing-chip.

31 "FAA Needs to Address Weaknesses in Air Traffic Control Systems," GAO, January 2015, http://www.gao.gov/assets/670/668169.pdf.



Source: IOActive Labs.

discussing ways to provide this security service to aircraft in flight to warn pilots of a potential cyberattack.

But corporate IT approaches to cybersecurity tend to have higher rates of failure than critical aviation systems would support, and may be otherwise ill fit for an aviation environment. As stakeholders consider using SOC services to monitor aircraft and aviation operations, they will encounter challenges. It may be difficult to capture weak signals in a sea of data, tune monitor for effectiveness, and minimize false negatives or false positives on airborne platforms. Additionally, the time span of adversary activity, SOC response, reaction, and communication may pose a challenge to offering timely information. To partially overcome the challenge of SOC reach-back, the potential for a degree of autonomous onboard network 'intrusion detection' has already been researched.[32] Such a model of remote/autonomous monitoring is arguably what protects many networks around the word. The difficult question is whether such a model is robust enough to protect live aviation systems and if the industry wants aviation operators (pilots, air traffic controllers, etc.) to become part of the cyber incident response team.

Passenger Services

The airline industry has come a long way from the days of nonexistent passenger connectivity. In 1984, airlines offered the first public air-ground pay telephones with Airfone. At the time, it was assessed that 20 to 30 percent of airline passengers were interested in the service and that public demand would determine how the service evolved.[33] Looking across the industry today, it is safe to say that public demand for connected services is not in question.

Over the last two years, the number of airlines offering in-flight Wi-Fi has increased by 38 percent and the chances of passengers boarding a Wi-Fi equipped aircraft is 39 percent.[34] This market is

32 Silvia Gil-Casals, "Risk Assesment and Intrusion Detection for Airborne Networks," Networking and Internet Architecture [cs.NI], INSA Toulhouse, October 20, 2014, https://hal.archives-ouvertes.fr/tel-01075751.

33 Stuart Diamond, "Now, Pay Phones on Jetliners," *The New York Times*, October 15, 1984, http://www.nytimes.com/1984/10/15/business/now-pay-phones-on-jetliners.html.

34 *2017 Wi-Fi Report*, Routehappy, 2017, https://www.routehappy.com/insights/wi-fi/2017.

Airliner cabin with IFE. *Photo credit:* Constanza Sturm/Flickr.

quickly evolving from offering basic connection to the regular use of personal devices while onboard. The growth of onboard Wi-Fi is not just for delivering content; it also provides airlines an opportunity to engage with passengers and capitalize on more services. It is not just passengers that are exploiting the digital revolution within the aviation industry, increasingly airlines and aircraft manufacturers are too.

Aircraft Services

The worldwide growth in cockpit and aircraft system connectivity has created a plethora of additional services that are proving important to the aviation industry. The following sections highlight a number of these technologies, their benefits, and potential issues when it comes to securing an increasingly complex ecosystem.

Electronic Flight Bags

The complexity of aircraft and airspace has increased the amount of information that aircrew need to access during flight. Flight charts, maps, aircraft engineering documents, and much more used to be carried on bulky and heavy paper in a physical flight bag. As technology became smaller, the aspiration to develop a paperless cockpit took hold. Initially, this took form as a simple, standalone, portable electronic display device that simply stored paper information in electronic format. After initial successes and positive feedback, the functionality and external interfaces on these Electronic Flight Bags (EFB) grew as the technology evolved. Now, the most sophisticated EFBs have bidirectional interfaces with the aircraft, external data sources, and video surveillance displays (such as the security camera covering the cockpit door). Their growing usefulness is such that they are now used to calculate performance (takeoff) data and to host regulated and unregulated software in different data enclaves. As their usefulness and ubiquity grow, sophisticated EFBs are being built into aircraft cockpits.

Companies applying to incorporate EFBs are required by the European Aviation Safety Agency (EASA) to demonstrate that "adequate security procedures are in place to protect the system" and guarantee that "prior to each flight the

EFB operational software works as specified."[35] Connectivity between the aircraft and a portable EFB is specifically highlighted as being critical to security standards, increasing in importance the closer the EFB is to critical systems. Therefore, data transmission is limited to systems that have:

- no safety effect or minor safety effects on the aircraft;
- been certified to connect to the EFB; and
- are completely isolated from aircraft systems.

These limitations along with additional suggestions, such as securing EFBs through the likes of firewalls, virus scans, and up-to-date software, are good basic advice, but may not encompass the entire attack surface. As their growth in popularity has increased, the variety of hardware and software used for portable EFBs has also increased. Diversity and platform complexity may make it harder to demonstrate assurance and deliver reliability. Already there have been incidents such as third-party applications crashing aircrew EFB tablets and forcing aircrew to print maps as well as the virus that propagated across EFBs used by Thai Airways in 2007.[36]

A key stage of preparing an aircraft for takeoff is calculating the performance required for takeoff. To save fuel and minimize engine wear and noise, full engine power is only used when and if required. So, if the runway length, aircraft, and environmental factors permit a safe takeoff, a calculated power setting less than 100 percent will be used. Determining that figure correctly is critical.

The implications of getting it wrong were demonstrated in 2004, when an MK Airlines Boeing 747, using a system similar to an EFB, crashed during takeoff. Investigators suspected that the crew had somehow miscalculated or misread the data presented by the electronic source, failed to double check it, and subsequently used it, leading to the crash.[37] Although in this case there was no malicious intent in the incident, and safety processes should have caught the error, it is a salutary reminder of the importance of protecting the information presented to aviation industry operators and decision-makers.

Aircraft Communications Addressing and Reporting System

An Aircraft Communications Addressing and Reporting System (ACARS) is a digital air-to-ground communication capability that can use a number of links such as ground-based Very High Frequency (VHF)/high frequency or Inmarsat/Iridium Satellite Communications (Sat Comm). Although seen primarily as an aircraft to airline operator method of communication, its transition into a VHF digital link means that both its bandwidth and speed have increased and as such is increasingly used to carry Air Traffic Control (ATC) communications.[38]

As an unencrypted, openly transmitted messaging system, ACARS cannot be considered secure. Although an encryption standard for ACARS was developed, ACARS message security is inconsistent in its uptake.[39] Other proprietary ACARS encryption 'add-ons' have been developed, but many are considered highly insecure and give no more than an illusion of security.[40]

Therefore, observing and decoding ACARS has become a surprisingly easy pastime for many enthusiasts and researchers. With little hardware and software from the Internet, they can both receive and transmit on ACARS channels. On the face of it, as an open data-link, the main issue with ACARS would be privacy maintenance, but as cockpit interconnectedness has increased, the potential threat has been elevated to something potentially more concerning.

Many aircraft now have ACARS fitted into the cockpit with connectivity to aircraft systems, predominately the Flight Management System (FMS). The FMS manages navigation routes, databases, airfield details, etc., and is an essential part of operating a modern airliner. As ACARS can be used to transmit the flight plan to the aircraft, it is very common to have the ACARS connected to the FMS. When a flight plan arrives on the ACARS,

35 "Annex II - AMC 20-25," EASA, September 2, 2014, https://www.easa.europa.eu/system/files/dfu/2014-001-R-Annex%20II%20-%20AMC%2020-25.pdf.

36 Darlene Storm, "What Third-Party App Crashed American Airlines Pilots' iPads and Caused Flight Delays?" *Computerworld*, April 29, 2015, https://www.computerworld.com/article/2916577/security0/what-third-party-app-crashed-american-airlines-pilots-ipads-and-caused-flight-delays.html; R. De Cerchio and C. Riley, "Aircraft Systems Cyber Security," *30th Digital Avionics Systems Conference*, IEEE, October 16-20, 2011.

37 Linda Werfelman, "Fatal Calculation," *Aviation Safety World*, October 2006, https://www.flightsafety.org/asw/oct06/asw_oct06_p18-24.pdf.

38 "Data Link," Rockwell Collins, 2017, http://www.arincdirect.com/what-we-do/flight-deck-communications/data-link/.

39 Matthew Smith, et al., "Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS," Financial Cryptography and Data Security, 21st International Conference, April 2017, http://fc17.ifca.ai/preproceedings/paper_17.pdf.

40 Ibid.

Diversity and platform complexity may make it harder to demonstrate assurance and deliver reliability.

the pilot reviews it and, if desired, can upload it directly to the FMS.

Therefore, the link between the ACARS and FMS is a potential access point into aircraft systems. Hugo Teso, a cyber researcher and a commercial pilot, claimed that such a link enabled ACARS to be used as an attack pathway into aircraft systems, permitting compromise of everything to do with the "navigation of the plane."[41] Both the FAA and the EASA countered the allegations saying that they would not work in a real-world situation.

Teso is not the only one to take an interest in aircraft data links, and he will certainly not be the last. Simple counters that it will not work in the real world may not be enough to reassure stakeholders without also providing an explanation of why it will not work. As the next section shows, claims of exploitation are only likely to increase.

Aircraft Health Monitoring – Supporting the Aircraft

With the increasing pressures on airlines to maximize efficiency, aircraft Original Equipment Manufacturers (OEM) are striving to utilize connected technology to deliver more accurate AHM and predictive maintenance. Previously, aircraft parts would either be inspected on a scheduled maintenance plan, which requires costly and time-consuming dismantling of aircraft systems to inspect wear rates, or the parts would be left to fail, requiring repairs on short notice. Now, as thousands of aircraft parts and components are increasingly connected and able to feed data to AHM systems, large dataset analytics permit the maintenance team to conduct sophisticated analysis while the aircraft is in flight or on the ground.

This real-time data from the aircraft to the ground operations team is speeding up engineering and maintenance decision-making to the extent that plans can be developed while the aircraft is still in the air. This reduces the time taken to diagnose, fix, and return aircraft to flight, minimizing downtime and maximizing efficiency. With the vision for such systems to have entire airline fleets feeding data into data warehouses, which can then be analyzed by airlines and aircraft manufacturers, it is understandable to see such partnerships as Airbus with the analytics firm Palantir, both of which see the benefits of such a partnership stretching beyond aircraft data and into passenger data.[42]

Observed examples of connected AHM systems include engine-monitoring systems that will transmit aircraft and engine data via Global System for Mobile Communications (GSM), Wi-Fi, or satellite phone to a web interface. An installation using GSM must incorporate a GSM sim card into aircraft systems that can then be interfaced with the Internet to transmit data. It includes the capability to transmit data directly to EFBs, making data immediately accessible to aircrew. It also includes the capability for the aircraft to automatically connect to a Wi-Fi hotspot at the airport gate to download AHM data and upload In-Flight Entertainment (IFE) content. Although space limitations preclude in-depth analysis of individual systems, observations, and potential concerns, the overall perception is that the potential attack surface is considerable.

Aircraft Maintenance

It is also of utmost importance to secure both the aircraft and the surrounding maintenance systems. Servicing the aircraft is becoming increasingly technology-centric with such things as aircraft data being networked to maintenance team's handheld or augmented reality devices. Managing and securing this ecosystem of paperless processes and data transfers between the aircraft and ground systems will become a greater challenge. Although these risks may not be directly safety critical in nature, they absolutely contribute to maintaining safe operations, as demonstrated in a 2008 crash.[43] The direct cause of the crash was an attempt to takeoff while in the wrong configuration. The aircraft should have been grounded after three such failures, but the system warning for such errors was malfunctioning. The engineering computer that tracked such failures was allegedly infected with

41 "Cyber Threats against the Aviation Industry," InfoSec Institute, April 8, 2014, http://resources.infosecinstitute.com/cyber-threats-aviation-industry/; Hugo Teso, "Aircraft Hacking: Practical Aero Series," n.runs Professionals, April 2013, https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf.

42 "Deep Data: The Beating Heart of Flight," Airbus, press release, July 2017, http://airbus-xo.com/deep-data-beating-heart-flight/.

43 Deborah A.P. Hersman, "Safety Recommendation," NTSB, August 17, 2009, https://www.ntsb.gov/safety/safety-recs/recletters/A09_67_71.pdf.

malware that slowed down the identification of the issue.[44] The malware did not cause the crash, but it removed a crucial safety break that could have prevented the aircraft from taking off.

In an environment where adversaries will look to create harm, compromise of safety breaks must be assumed as a potential risk. In the previously discussed crash, although the malware is thought to have been non-targeted, similar targeted activity with motivations to disrupt, confuse, and obfuscate, become a critical matter to understand and counter.

The Challenges

One of the most telling things that came out of the research for this report was the variety of challenges that will come with the connected aircraft of the future. The scale of the challenge cannot be underestimated.

In the days before 'connected aircraft,' a passenger connecting a device to an aircraft would have been anathema to many in the aviation industry. Even as consumers have become increasingly aware of cyber vulnerabilities in other industries, aviation has had a comparatively quiet period. But stories, claims, and studies are raising the potential issues associated with passenger connectivity. A high-profile claim in 2015 changed the tempo when Chris Roberts, a cybersecurity researcher, claimed to have adjusted an airplane's engines by connecting to the IFE unit beneath his seat. His tweet about his actions resulted in questioning by the Federal Bureau of Investigation and government and industry subsequently spending an estimated $14 million to investigate and refute the claims.

Also in 2015, a researcher at IOActive observed software debug information on his IFE screen while airborne. On landing, he discovered that multiple versions of the IFE software were freely available online. After investigating, his conclusion was that it may have been possible to compromise the IFE and disconcert passengers through manipulation of lighting, displayed information, etc.[45]

That same year, Hugo Teso responsibly disclosed the findings of a yearlong study into aircraft system vulnerabilities to EASA. His central tenet was that he had found a series of backdoors into aircraft systems that were remotely exploitable. The response from the aviation industry audience was allegedly unanimous: "You aren't really planning on making all of that public, are you?"[46]

With increased technology and connections around and onboard aircraft, the curious, mischievous, and malicious will attempt to explore it as an attack surface, not only with Wi-Fi but also with any RF signal or access point on the aircraft. Evolution is happening quickly, not just with those attempting to compromise aircraft systems, but also with passengers attempting to compromise the cybersecurity of other passengers.[47] In moving forward, understanding this multi-faceted attack surface, how to secure it, and how to assure it will be essential.

Understanding and Securing an Expanding Attack Surface

Many contributors to this report agreed that the aviation industry's rapid technological adoption of hardware, software, and a complex supply chain have dramatically increased both the attack surface of systems that could be affected and the potential ways of affecting them. Arguably, defining a potential attack surface will be based on perceptions. A determined attacker will seek an attack surface where none may have been perceived by the defender. Adversaries may even chain together disparate vulnerabilities until they can create an attack surface. For example, when an adversary allegedly stole aircraft designs from a US defense contractor, the attack surface may have been created by stealing two-factor authentication data from another company.[48]

The high number of airline systems interacting with aircraft must be considered a large part of the attack surface that could provide a single point of entry to a multitude of aircraft. The more seamless the system between the aircraft and the airline, the more that such a system must be considered critical. Proactively finding a potential attack surface and exploring what may be possible is a key task for the aviation industry. Long-term solutions will come from considering both defender and adversary

44 Leslie Meredith, "Malware Implicated in Fatal Spanair Plane Crash," NBC News, August 20, 2010, http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/#.WdMpZmhSyUk.

45 Ruben Santamarta, "In Flight Hacking System," IOActive, December 20, 2016, http://blog.ioactive.com/2016/12/in-flight-hacking-system.html.

46 Marcel Rosenbach and Gerald Traufetter, "Hackers Warn Passenger Planes Vulnerable to Cyber Attacks," *Spiegel Online*, May 22, 2015, http://www.spiegel.de/international/business/hackers-warn-passenger-planes-vulnerable-to-cyber-attacks-a-1035172.html.

47 Steven Petrow, "I Got Hacked Mid-Air While Writing an Apple-FBI Story," *USA Today*, February 24, 2016, https://www.usatoday.com/story/tech/columnist/2016/02/24/got-hacked-my-mac-while-writing-story/80844720/.

48 Angela Moscaritolo, "RSA Confirms Lockheed Hack Linked to SecurID Breach," *SC Media*, June 7, 2011, http://www.scmagazine.com/rsa-confirms-lockheed-hack-linked-to-securid-breach/article/204744/.

perceptions, rather than discounting or attempting to obscure a potential attack surface.

Security Through Obscurity

Aviation industry adversaries have had a relatively steep learning curve due to the obscurity of access and knowledge. However, increases in interoperability, corporate IT practices and technologies, and convergence of networks may quickly erode "security through obscurity."

In cryptography, if a cryptographic methodology can be independently examined and tested for its security, it is possible to not only assure its security but also demonstrate its security. Currently, assessing how secure aircraft systems are is a challenge. From interviews, the connectivity of aircraft systems and how they are secured is very often protected information. It can be argued that a degree of obscurity in secure system design can add a layer of challenge and delay to adversary interference, but it can only be considered one (thin) layer of a multi-layer system.

Additionally, the greater the role obscurity plays in protecting a system, the greater the impact when that obscurity is compromised. Whether system or network designs are accidentally or deliberately compromised, once they are openly available, the underlying architecture must be resilient enough to continue protecting the system in question.

The more visibility the security methodology has, the more that multiple perspectives can assess and advise on its resilience. There is a balance to be had, but the aviation industry cannot quickly refine the security of aircraft systems with obscuring methodologies that may slow wider, valuable collaboration.

Independent Assessment and Vulnerability Management

The aviation industry has long understood the value of independent assessment and the assurance of safety critical systems. Losing that independence or rigor has arguably resulted in a number of major aviation accidents.[49] The value of independent assurance and cybersecurity assessment is arguably equally important for connected aircraft. In other industries, independent assessment through such things as penetration tests, white/grey/black box testing, red teaming, etc. is increasing in value and depth.[50] Such activity does not just evaluate the people, processes, and technologies involved, it also tests the assumptions of the risk owner.

Several manufacturers and suppliers are now starting to employ some form of independent vulnerability assessment program to find and fix vulnerabilities before they become common knowledge. Although many of these programs are 'by invite' only, it is hoped that these will increase in scale, ambition, and sophistication as the industry evolves. The more diversity in knowledge, ability, and creativity that contributes to such activity, the better. The relationship between independent cybersecurity researchers and the aviation industry up till now has been poor. Building trust and relationships can only be a good thing for increasing cybersecurity and safety across the aviation industry and, though it may take time, must be prioritized.

Future Networks

After concern that ACARS and other such supporting systems are aviation unique, the aviation industry has initiated a project to modernize them.[51] The objective is to develop an aviation Internet Protocol Suite (IP Suite) based on current network technology (e.g., TCP, User Datagram Protocol, Internet Protocol version 6 [IPv6]). By increasing standardization, it is hoped that increased use of commercial off-the-shelf components may be possible.

As the development of IP Suite accelerates, there is much to learn from the current crop of datalink vulnerabilities increasingly coming to the fore. There are already discussions about whether IP Suite could be used to secure and transmit safety services over data networks primarily intended for cabin services.[52] As aircraft data generation increases, finding methods to securely get that data off the aircraft will be a challenge.

Conceivably, the demonstrably safe and secure way to segregate the different sets of data from different domains would be to have individual bearers and hardware for every domain. Such an approach brings impacts in the form of replicating hardware, and therefore cost and weight. Additionally, the bearer of choice will vary depending on the phase

49 For example, read about the loss of Nimrod XV230 in Charles Haddon-Cave, *An Independent Review Into the Broader Issues Surrounding the Loss Of The RAF Nimrod MR2 Aircraft XV230 In Afghanistan in 2006,* London: The Stationary Office, Tech. Rep., October 28, 2009, *doi:HC1025.*

50 Girish Janardhanudu and Ken van Wyk, "White Box Testing," US-CERT, July 5, 2013, https://www.us-cert.gov/bsi/articles/best-practices/white-box-testing/white-box-testing#BandG.

51 "ARINC Project Initiation/Modification (APIM): Internet Protocol Suite for Aeronautical Safety Services – Development Plan," AEEC, September 23, 2015, http://www.aviation-ia.com/aeec/projects/ips/Apim15_004.pdf.

52 Mary Kirby, "Will Safety Service Ever Transmit over Cabin Connectivity Pipes?" *Runway Girl*, October 12, 2017, https://runwaygirlnetwork.com/2016/10/12/will-safety-service-ever-transmit-over-cabin-connectivity-pipes/.

of flight, comparative cost, and available speed. Sat Comm will be the only mid-ocean option: overland has the option of air-to-ground links and airports have the option of wireless networks. Sharing links between safety critical and non-safety critical services may be the pragmatic solution, but finding a solution to secure and assure them may be harder, for as soon as data from different domains is transmitted over the same bearer, a declared position of absolute segregation is considerably more difficult to demonstrate.

What is certain is that whatever decisions are made about aircraft security, adversaries will assess potential vulnerabilities as much as the aviation industry.

A Balancing Act – Threat, Design, Assurance

If it is accepted that connected aircraft are now potential targets for cyber adversaries, the threat model for the aircraft design must be considered early in the process. As the threat model evolves over time, it may be difficult to accommodate new threats into the project design.

Manufacturers must design to regulated standards of assurance and security, but with aircraft in design, production, and operation for years, defining benchmarks to appropriately balance risks in the long term is a challenge. Many nations and organizations are looking at this problem. In the United States, the FAA set up the Aircraft Systems Information Security/Protection (ASISP) working group in 2015 with aims to provide advice and recommendations on "ASISP-related rulemaking, policy, and guidance, including both initial certification and continued airworthiness."[53]

A key strength of the ASISP working group is that the scope includes not just airplanes but also rotorcraft—recognizing that the technologies, and therefore challenges, across fixed and rotary platforms are similar. Incorporating UAS and commercial passenger space operations to their scope would additionally make the working group even more comprehensive. Other organizations, such as the Radio Technical Commission for Aeronautics, assist in developing aircraft standards consensus around 'aviation modernization issues.'[54] This means that their Special Committee 216 on aeronautical systems security ends up on the front line of collaboration and development of ASISP regulations both in the United States and in Europe. Examination of their work through published minutes shows considerable effort and dialogue in moving regulation forward, but the issue remains complex.

Irrespective of threat model or legislation, the intricate and complex nature of the supply chain and its governance brings another challenge: that of tracking components and software. As vulnerabilities are discovered and cybersecurity legislation or threat models changed, being able to quickly identify all affected components and software will be essential to quickly understanding and mitigating risk. Where the responsibility of that risk sits will need discussion and agreement across the entire ecosystem.

The increased complexity of components and software means that legislation such as the Internet of Things (IoT) Security Improvement Act of 2017 will be key.[55] By mandating secure patching, absence of hard-coded passwords, and no known vulnerabilities, responsibility is placed on the supplier to better protect the customer. Some may consider such legislation onerous, but when so much of aviation security sits at the component level, this may be one of the few ways to quickly course correct suppliers to remove entire classes of vulnerability.

The balance between threat, system design, and regulation is a difficult undertaking, not only because the different elements are hard to capture and often evolve at varying rates, but also because the threat frequently outpaces system design and regulation. In such a situation, incremental improvement may not be sufficient—especially as aircraft systems are increasingly connected and developed. There is a strong argument that in addition to finding and patching vulnerabilities, efforts must focus on removing entire classes of vulnerability—in effect, seeking to reduce the complexity space.

53 "Aircraft Systems Information Security/Protection (ASISP) Working Group," FAA, 2015, *Federal Register* 80 (22): p5880–82.

54 "About Us: Overview," RTCA, https://www.rtca.org/content/about-us-overview,

55 US Congress, Senate, Committee on Homeland Security and Governmental Affairs, *Internet of Things (IoT) Cybersecurity Improvement Act of 2017*, 115th Cong., 1st sess., 2017, https://www.congress.gov/115/bills/s1691/BILLS-115s1691is.pdf.

UNMANNED AIRCRAFT SYSTEMS

Commercial UAS capabilities are growing quickly, and increasingly larger unmanned aircraft are being used for roles such as surveillance and cargo. While there is currently little appetite for large-scale pilotless passenger services, unmanned cargo aircraft or smaller pilotless transport aircraft are also being developed. Exploring the cybersecurity and safety aspects of this sector is important, as carriers will not only have to demonstrate that they can operate safely, but that they can do so in congested airspace surrounded by other aircraft.

As of August 2017, an unmanned MQ-9B conducted an FAA approved flight through "multiple classes of non-segregated airspace."[1] As the UAS industry evolves, full integration with manned aircraft in controlled airspace is now considered a distinct possibility. With potential threats to both the platform and the ATM system, doing this safely will be a considerable challenge.

Growth – Scale and Diversity

The number and diversity of air platforms without a human operator directly at the controls are due to rapidly increase. Whether it is the Facebook Aquia long endurance UAS, which will fly above commercial airspace but still past through it; the K-Max unmanned heavy lift helicopter, the Natilus 777 sized platform that will autonomously carry 20,000 lbs. of goods across the world; or the plethora of autonomous and semi-autonomous 'flying car' concepts that are under development (including a flying taxi), coordination of safety standards and operational protocols is of the utmost importance.[2]

A strategy to secure these platforms must focus on both the safety of the individual UAS operations and the continued safety of pre-existing aviation industry operations. This will not be a simple task. As systems become more common and add greater value, the motivation for adversaries to seek out opportunities to attack will burgeon.

As the capabilities of the UAS industry advance, the nuance between autonomous versus unmanned will also become increasingly important—especially when things go wrong. Currently, an individual UAS pilot when faced with a potential emergency only has to focus on one aircraft. As the industry develops more 'autonomous' platforms, one operator might be managing multiple aircraft. In a world where cyber adversaries care not about autonomous or unmanned, being able to safely operate through adversity irrespective of scale will be a complex challenge.

Challenges and Opportunities

Because a great deal of early UAS platforms are military in nature and operating in a high threat environment, incidents such as the downing of an apparently intact RQ-170 by Iran and the keylogger discovered in UAS control systems at Creech Air Force Base, have spurred the defense industry to consider the potential threats.[3] The US Department of Defense and the FAA invited researchers from the University of Texas to the White Sands Test range where they successfully spoofed the Global Positioning System (GPS) signal of a civilian unmanned aerial vehicle and subsequently commandeered it.[4]

No matter what a UAS looks like, it is fundamentally a node on a network that accepts commands. While these commands normally originate from the designated operator, researchers from Johns Hopkins University discovered no less than three different exploits that caused a UAS to make an uncontrolled landing.[5]

---

1 Courtney E. Howard, "MQ-9B SkyGuardian Conducts FAA-Approved Flight through Multiple Classes of Non-Segregated Airspace," *Intelligent Aerospace*, August 23, 2017, http://www.intelligent-aerospace.com/articles/2017/08/mq-9b-skyguardian-conducts-faa-approved-flight-through-multiple-classes-of-non-segregated-airspace.html.

2 "K-MAX," Lockheed Martin, http://www.lockheedmartin.co.uk/us/products/kmax.html; "Natilus," Natilus, http://www.natilus.co/; Rodin Lyasoff, "Welcome to Vahana," Vahana, Airbus, September 23, 2016, https://vahana.aero/welcome-to-vahana-edfa689f2b75.

3 John Keller, "Iran–U.S. RQ-170 Incident Has Defense Industry Saying 'Never Again' to Unmanned Vehicle Hacking," *Military Aerospace*, May 3, 2016, http://www.militaryaerospace.com/articles/2016/05/unmanned-cyber-warfare.html.

4 "Cockrell School Researchers Demonstrate First Successful Spoofing of UAVs," University of Texas at Austin, press release, June 27, 2012, https://www.engr.utexas.edu/features/humphreysspoofing.

5 "Johns Hopkins Team Makes Hobby Drones Crash to Expose Design Flaws," Johns Hopkins University, press release,

These demonstrations and the RQ-170 incident highlight the significant challenges that the UAS industry may be facing. The personal and commercial UAS market is already valued at $6 billion in 2017 (with three million new UAS expected to be produced in 2017) and forecasted to reach $11.2 billion in 2020.[6] While the aviation industry is facing a considerable challenge regarding how to integrate and regulate UAS, there will also be a key requirement to further develop security and resilience.

Such a challenge is far from a solo voyage of discovery for the aviation industry. With autonomous vehicles in development for both ground and sea, there are many opportunities for cross-collaboration and learning, which may accelerate understanding across all industry verticals.

June 8, 2016, http://releases.jhu.edu/2016/06/08/johns-hopkins-team-makes-hobby-drones-crash-to-expose-design-flaws/.

6 "Gartner Says Almost 3 Million Personal and Commercial Drones Will Be Shipped in 2017," Gartner, press release, February 9, 2017, https://www.gartner.com/newsroom/id/3602317.

Air Traffic Management

SECTION TAKEAWAYS

- 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.
- Using advanced technologies such as GPS and Automatic Dependent Surveillance – Broadcast (ADS-B) can greatly improve accuracy and reliability, yet they remain susceptible to degradation by both environmental hazards and adversaries.
- When next generation ATM systems are presented with failure or adversary interference, the use of legacy capabilities as a backup will permit safe operations but at the cost of capacity.

> "For ATM, a number of guiding principles should be defined for the organizational and technical measures that are needed to encourage cyber resilience. These must recognize that organizations and technical systems will suffer from cyber incidents and attacks, and there is a possibility that some attacks in the future may be successful."
>
> European ATM Master Plan 2015 [56]

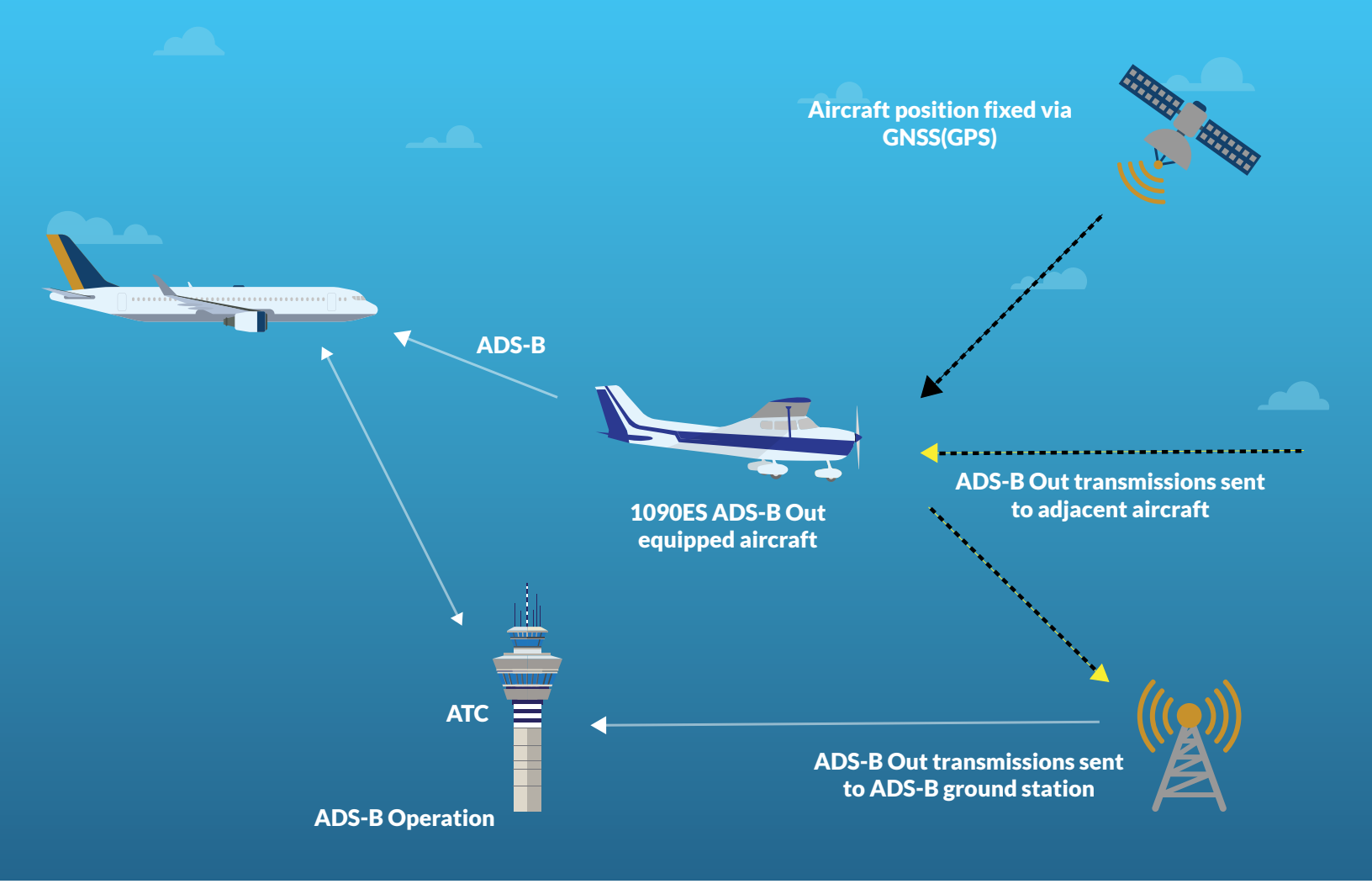
Managing and segregating aircraft in the early days of aviation was not much of an issue as there were not many aircraft to oversee. As numbers increased, procedural deconfliction eventually gave way to radios and radar, which is basically where the technology and processes sat for many years. Although there have been capability updates, traditional ATM infrastructure is now creaking under the load of increased global air traffic. There can be around fifteen thousand aircraft in the skies at any given moment. This is becoming even more difficult to manage with air traffic doubling every fifteen years on average.[57] As aircraft range also increases, routes often now extend over oceans with little in the way of radar coverage.

As demand starts to outstrip airspace capacity, it can lead to unpredictability, delays, and congestion. Inclement weather and other distractions only exacerbate the challenge. For airlines attempting to maintain tight timescales and small margins, unexpected events can reverberate across the entire operation—forcing aircraft to divert, taking days to recover, and impacting both the environment and the bottom line.

Efforts to modernize ATM will go a long way in mitigating many of these issues and create capacity

56 The Roadmap for Delivering High Performing Aviation for Europe: European ATM Master Plan, SESAR, 2015, https://ec.europa.eu/transport/sites/transport/files/modes/air/sesar/doc/eu-atm-master-plan-2015.pdf.

57 *Growing Horizons.*



Source: FANS-1/A Operations Manual and Trig Avionics Limited.

and flexibility. The following sections explore the future of ATM, some of the systems it is using, and some of the challenges it may face.

Improving Capacity and Efficiency

Due to increasing concern about aircraft management capabilities, the ICAO launched a committee on Future Air Navigation Systems (FANS) in 1983 to look twenty-five years ahead. After the committee's subsequent report and endorsement, the FANS concept evolved into what is known as Communications, Navigation, and Surveillance (CNS)/ATM systems.[58] After a number of national and regional initiatives to develop new CNS/ATM systems, it was "recognized that technology was not an end in itself and that a comprehensive concept of an integrated and global ATM system, based on clearly established operational requirements, was needed." The ICAO then developed and published a Global ATM Operational Concept in 2005 that became the foundation of many initiatives in progress today.[59]

This concept and its improvements across communications, navigation, and surveillance are under development globally. For example, in the United States, the FAA took the concept forward as Next Generation Air Transportation System (NextGen) and Europe has dubbed it the Single European Sky ATM Research (SESAR). Much of the discussion around future ATM systems can be applied laterally since the aims and concepts of the above initiatives are roughly similar.[60] It is arguably the largest and most sophisticated transformation of ATM in its history and will have a number of broad benefits.

Michael Huerta, Deputy Administrator of the FAA, discussed the following benefits of the transformation:

- Safety Improvements in Situational Awareness (SA) for pilots and air traffic controllers through

58 "International Civil Aviation Organization Global Air Traffic Management Operational Concept," ICAO, 2005, https://www.icao.int/Meetings/anconf12/Document%20Archive/9854_cons_en[1].pdf.

59 Ibid.

60 Elinor Ulfbratt and Jay McConville, "Comparison of the SESAR and NextGen Concepts of Operations," NCOIC, May 2008, https://www.ncoic.org/images/technology/whitepapers/SESAR_NextGen_Comparison_20090317FINAL.pdf.

increased use of automation, data fusion, and Data Communications (Data Comm).

- Environmental Saving time, fuel, and reducing noise through either direct routing or pruning the time aircraft spend in level flight by means of continuous descent profiles.
- Airports Improve SA and traffic flows to produce a more predictable and efficient service.
- Flight Operations Firstly, in the category of 'efficiency and capacity,' aircraft safe separation distances can be reduced, weather impacts minimized, flight plans and routing options expanded, and SA improved. Secondly, in the category of 'access,' greater SA will make runway operations and airport arrivals and departures more efficient.[61]

In the United States, the transformation of ATM is already yielding monetary profits. With the initial systems already online and an increasing number of pilot programs, the FAA estimates that NextGen has delivered $2.7 billion in benefits between 2002 and 2017, with that number estimated to increase to $161 billion by 2030.[62]

The Air Traffic Management Ecosystem

To deliver these benefits, a new generation of ATM systems will increasingly replace their legacy equivalents. For example, some key systems are highlighted below:

- System Wide Information Management (SWIM) This is to become the IP digital backbone/ architecture for the global movement of ATM data. It moves away from bespoke, point-to-point communications on multiple systems to a single point of access for all aviation data—an ATM global intranet.
- Data Comm This is a system of data links and systems that create a digital link between the ground and flight deck avionics. It permits a shift away from voice communications between ATC and aircraft, improving ATC information for airline operations. Data Comm can be used for such things as safety of flight messages, clearances, instructions, requests, and reports.[63] As the program matures, enhanced capabilities will permit received messages to load automatically into the aircraft FMS on pilot request.[64]

Within Data Comm, the following two systems are of key interest:

- Automatic Dependent Surveillance – Broadcast This transforms the architecture of how air traffic controllers manage aircraft. Previously, aircraft positioning was derived procedurally or from radar. With ADS-B, aircraft broadcast their GPS position and other data. ADS-B has two different services, ADS-B 'out' is where aircraft broadcast GPS location and other information but do not receive data. With ADS-B 'in,' as well as broadcasting, aircraft receive ADS-B information from ground units and other ADS-B aircraft, effectively giving ADS-B 'in' aircraft the same SA display of ATC.[65]
- Controller-Pilot Data Link Communications (CPDLC) Whereas ACARS was for communications between the aircraft and 'company,' CPDLC is primarily for digital messaging (similar to sending a text) between the air traffic controller and the pilot. CPDLC will increasingly replace traditional voice communications.

The Challenges

Even before the development of NextGen and other technologies, ATM experienced interference activities such as the spoof radio calls around Melbourne in 2015 that caused a number of problems and forced at least one aircraft to abort its landing.[66] Although safety was not compromised, both the police and aviation organizations involved had to spend considerable time reassuring the public. Radios are cheap, difficult to track, and can cause

61 Michael Huerta, "The Benefits of the Next Generation Air Transportation System," Statement to the Committee on Transportation and Infrastructure, Subcommittee on Aviation, US Department of Transportation, October 5, 2011, https://www.transportation.gov/content/benefits-next-generation-air-transportation-system.

62 "NextGen Update: 2017," FAA, 2017, https://www.faa.gov/nextgen/update/.

63 "Data Communications (Data Comm)," FAA, https://www.faa.gov/nextgen/programs/datacomm/.

64 "RTCA SC-214 / EUROCAE WG-78: Advanced Data Communication Baseline 2 Standards," EUROCAE RTCA, March 2013, https://www.icao.int/APAC/Meetings/2013_FIT_Asia2_RASMAG18/WG78-SC214%20Baseline%202%20Tutorial%20-%20Final%20(25March2013).pdf.

65 "14 CFR Part 91. Automatic Dependent Surveillance – Broadcast (ADS–B) Out Performance Requirements To Support Air Traffic Control (ATC) Service," FAA, May 28, 2010, *Federal Register* 75 (103). https://www.gpo.gov/fdsys/pkg/FR-2010-05-28/pdf/2010-12645.pdf.

66 "Police Issue Warning about Unauthorised Radio Transmissions at Melbourne and Avalon Airports," Australian Federal Police, press release, November 7, 2016, https://www.afp.gov.au/news-media/media-releases/police-issue-warning-about-unauthorised-radio-transmissions-melbourne-and.

disproportionate outcomes, which exemplifies the challenges facing the industry as it moves forward.

The technology behind future ATM was conceived during a period when adversary interference was not considered credible or even possible. In a world where computing power and Software Defined Radios (SDR) are cheap and powerful, and GPS jammers are easily available online, adversary ability to interfere has evolved rapidly.

A number of organizations, researchers, and contributors to this report raised concerns over the potential for unauthorized interference to various elements of future ATM systems. At a national level, the US Government Accountability Office (GAO) has also published a number of reports highlighting their concerns across ATM (NextGen), GPS, and ATC systems.[67] The following sections highlight some of these potential challenges and concerns. While an attack against one of the following elements may be cause for concern, as threats and capabilities against the aviation industry mature, the greater concern is the potential for adversaries to cause multiple safety critical failures by coordinating activity across multiple elements.

Space-Based Elements

Space-based capabilities are essential to rolling out ATM updates around the world. NextGen ATM and similar systems are dependent on Global Navigation Satellite Systems (GNSS) for Positioning Navigation and Timing (PNT). GNSS is so widely accessible and reliable that users generally do not worry about losing it or suffering degraded service. As a low power signal, however, it is highly vulnerable to interference from ground-based jamming and spoofing. Additionally, the increase in Sat Comm by aircraft for both passenger and aircraft services creates additional data-links that require securing.

Traditional external navigation aids for aircraft can largely be grouped into those that help navigation and those that help landing. Navigation beacons are ground-based transmitters that give the aircraft range and bearing from a known point. Landing beacons give very accurate range, azimuth, and elevation angles down to the runway threshold. With the advancement of GPS and the movement to replace legacy ground-based transmitters, there is a large drive toward using GPS guided Performance Based Navigation (PBN) for every aspect of the flight. The FAA's long-term goal is to make PBN the standard method of navigation and to reduce legacy navigation infrastructure.[68]

If the increased reliance on GPS for PBN is undisputed, neither are the potential vulnerabilities of GPS. In addition to the sophistication of GPS spoofing and the potential outcomes against UAS that have already been discussed, there are wider challenges worth exploring. In 2013, the GAO published a paper on the "risks and potential effects from disruptions in the GPS on critical infrastructure."[69] This paper highlighted that GPS can be degraded through natural (e.g., space weather), accidental, or intentional means. Concern about accidental error was recently demonstrated when a thirteen microsecond timing discrepancy, caused by a satellite taken out of service, impacted users globally for around twelve hours.[70]

The ease of procuring GPS jamming equipment, even though their use is widely illegal, makes intentional jamming of the GPS signal a key concern for the aviation industry. This was highlighted in August 2013 when Newark Liberty International Airport's PNT systems suffered interference from a low-cost mobile jammer.[71]

Jamming the GPS signal used to be the predominant method of intentional GPS disruption, but it is concerning that sophisticated spoofing on a larger scale is being seen more frequently. Over twenty vessels reported GPS location errors during an incident in the Black Sea. One ship showed its location as twenty-five miles inland with a GPS accuracy of less than one hundred meters for several days. Additionally, the automatic identification system, which vessels use to transmit their location to other vessels, was showing a number of 'ghost ships.'[72] Wide-area augmentation

67 "FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen," GAO, April 14, 2015, https://www.gao.gov/assets/670/669627.pdf; "GAO-14-15, GPS Disruptions: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced," GAO, November 2013, http://www.gao.gov/assets/660/658792.pdf; "FAA Needs to Address Weaknesses in ATC Systems."

68 "Performance Based Navigation: PBN NAS Navigation Strategy 2016," FAA, 2016, https://www.faa.gov/c/content/dam/faa/nextgen/resources/PBN_NAS_NAV.pdf.

69 "GPS Disruptions."

70 Chris Baraniuk, "GPS Error Caused '12 Hours of Problems' for Companies," BBC, February 4, 2016, http://www.bbc.co.uk/news/technology-35491962.

71 Marlene H. Dortch, "Notice of Apparent Liability for Forfeiture," FCC, August 1, 2013, https://apps.fcc.gov/edocs_public/attachmatch/FCC-13-106A1_Rcd.pdf; Glen Gibbons, "FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS," *Inside GNSS*, August 30, 2013, http://www.insidegnss.com/node/3676.

72 Dana Goward, "GPS Spoofing Incident Points to Fragility of Navigation Satellites," *National Defense Magazine*, August 22, 2017, http://www.nationaldefensemagazine.org/articles/2017/8/22/viewpoint-gps-spoofing-incident-points-to-fragility-of-navigation-satellites.

Photo credit: NATS - UK air traffic control/Flickr.

systems and ground-based augmentation systems, which transmit either space- or ground-based signals to correct GPS signal errors, may make it more difficult to spoof aviation systems, but this is yet to be assessed.

For the aviation industry as well as resilient PNT, the importance of secure Sat Comm is critical. As space-based communication capabilities become ubiquitous for all aspects of the aviation industry, the security of the links, satellites, and ground stations becomes inextricably linked with aviation cybersecurity.

The cybersecurity challenge for space assets is not a hypothetical one. A report from Chatham House highlighted that risks exist across the entire space ecosystem with threats originating from states, criminal elements, or individual hackers.[73] Therefore, when assessing aviation cybersecurity, it must be assumed that adversaries will seek to pivot through or compromise space assets in their endeavors and it must be considered like any other attack surface.

Automatic Dependent Surveillance – Broadcast

The advantages of ADS-B within NextGen have already been mentioned, but there are contrasting views on the potential security issues of ADS-B. An ICAO ADS-B Implementation and Operations guidance document notes that "there has been considerable alarmist publicity regarding ADS-B security," and that "to a large extent, this publicity has not considered the nature and complexity of ATC." It expands further to say, "careful assessment of security policies in use today for ADS-B and other technologies provide a more balanced view."[74] The ICAO assessment of ADS-B vulnerabilities released only to member states is categorized into threats to confidentiality, integrity, and availability. It

73 David Livingstone and Patricia Lewis, *Space, the Final Frontier for Cybersecurity?* International Security Department, Chatham House, September 2016, https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

74 "ADS-B Implementation and Operations Guidance Document," ICAO (Asia and Pacific Office), June 2017, https://www.icao.int/APAC/Documents/edocs/AIGD%20Edition%2010.pdf.

recommends that states make themselves aware of the issues, taking note "that much of the discussion of ADS-B issues in the Press has not considered the complete picture regarding the ATC use of surveillance data."[75]

This report cannot comment on what is contained in the list of ICAO ADS-B vulnerabilities since they were inaccessible, but the described ICAO position on some ADS-B security research appears to be dismissive. Other comments strike a similar tone when discussing potential ADS-B vulnerabilities, such as ". . . this issue has been thoroughly investigated and international aviation does have a plan," and "an FAA ADS-B security action plan identified and mitigated risks and monitors the progress of corrective action. These risks are security sensitive and are not publicly available."[76]

As an open system with no encryption, authentication, or integrity checks, the main researcher concern is that ADS-B signals could potentially be eavesdropped on, blocked or transmitted by adversaries. The capability can allegedly be had for a few hundred dollars with cheap SDR and easily accessible open source software. Much research has explored potential ADS-B vulnerabilities including jamming (mass or selected aircraft), signal insertion (mass or selected spoofing), replay attacks, and signal (location/trajectory) manipulation.[77]

Mitigations for attacks against ADS-B group either into securing the link or validating the location.[78] There are several potential options to secure the link. For example, some form of encryption or authentication between ADS-B units could be deployed, but would be challenging to manage. To validate the location of an ADS-B transmission, multilateration (MLAT) can be used, but only for ground-based units. MLAT uses the differential in ADS-B signal time of arrival between different receiving stations to calculate a location for the transmitting station, and permits a degree of correlation that can differentiate the real from the fake.

An additional mitigation to ADS-B vulnerabilities is to layer in legacy radar capabilities. This will give controllers a raw radar 'paint' that can be augmented by additional information such as secondary surveillance radar. Although an initial intent of NextGen was to reduce the numbers of ATC radars, this goal is being scaled back to maintain the option of a radar fallback. It is worth mentioning that the loss of ADS-B and a fallback to radar in busy airspace may create capacity challenges for controllers. They may suddenly find themselves using a legacy system that requires greater separation distances, potentially impacting landing and departure rates.

ADS-B hardware is increasingly fitted and networked with other aircraft systems, making it a potential entry point for adversaries. Already many ADS-B units available for sale have both Wi-Fi and Bluetooth connectivity to permit uploading software and to link with EFB software on portable tablets. The recent report of an ADS-B transceiver with a permanently open Wi-Fi hotspot despite having a technical standard order authorization (i.e., design and production approval) from the FAA, demonstrates that there may be more challenges to come.

A Traffic Collision Avoidance System (TCAS) will actively look for potential aircraft collisions. If it believes a collision is likely, it will either instruct the aircrew on how to avoid it or take command itself, using autopilot to fly what it calculates to be the most appropriate avoiding action. A potential future hybrid system discusses using passive ADS-B 'in' signals to monitor other nearby aircraft for possible collision risks. If they get too close, the TCAS system would switch to active transmissions to resolve the situation.[79]

However, with future ATM systems designed to permit a considerable reduction in aircraft separation, a traditional transponder-based avoidance system may struggle. Airborne Collision Avoidance System X (ACAS-X), a new avoidance system that utilizes probabilistic modeling and ". . . dynamic programming to determine the best

75 Ibid.

76 Heather Kelly, "Researcher: New Air Traffic Control System Is Hackable," CNN, July 26, 2012, http://edition.cnn.com/2012/07/26/tech/web/air-traffic-control-security/index.html.

77 Brad Haines, "Hackers + Airplanes: No Good Can Come of This," Defcon 20, https://korben.info/wp-content/uploads/defcon/SpeakerPresentations/Renderman/DEFCON-20-RenderMan-Hackers-plus-Airplanes.pdf; Andrei Costin and Aurellien Francillon, "Ghost in the Air(Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices," Black Hat, 2012, https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf; Martin Strohmeier, et al., *OpenSky: A Swiss Army Knife for Air Traffice Security Research*, University of Oxford, September 13-17, 2015, https://www.cs.ox.ac.uk/files/7797/Strohmeier%20-%20DASC%202015%20-%20Paper.pdf.

78 Martin Strohmeier, "Security in Next Generation Air Traffic Communication Networks," University of Oxford, 2016, http://www.cs.ox.ac.uk/files/8693/Strohmeier%20-%20Security%20in%20Next%20Generation%20Air%20Traffic%20Communication%20Networks.pdf.

79 "Introduction to TCAS II, Version 7.1," FAA, February 28, 2011, https://www.faa.gov/documentLibrary/media/Advisory_Circular/TCAS%20II%20V7.1%20Intro%20booklet.pdf.

course of action. . .” is proposed for the future.[80] The ACAS-X system is also being designed so that it can take in and use multiple data sources, including ADS-B, to generate avoidance warnings and commands.[81] Any increased integration with aircraft collision avoidance systems and ADS-B must be very carefully considered. Adversaries attempting to cause ACAS to take avoiding action on false ADS-B signals is a potential threat that researchers have already highlighted.[82]

. . . [A]s a developing program, there are many details that still need to be worked out on how aircraft cockpits will be securely connected to a global intranet such as SWIM.

Controller-Pilot Data Link Communications

Like ADS-B, CPDLC is a data-link that is not encrypted or authenticated, making it potentially vulnerable to message manipulation, message injection, and spoofing of either ground elements or aircraft.[83] This could bring a number of challenges for operators as they attempt to detect subversion or maintain SA. If successfully conducted, subversion could permit an adversary to give instructions or requests to either ATC or aircraft. Aircrew and controllers can revert to voice communications to mitigate such an attack once suspected. The challenge is that, as has already been explored, spoofing voice ATC is cheap and accessible and CPDLC is essentially a digital version of voice. Both systems are therefore potentially vulnerable to the same effect. Not being able to use CPDLC would put controllers and aircrew back onto legacy voice communications already proven to be vulnerable and limited in capacity.

System-Wide Information Management

ATC services have already been a target of cyberattacks. For example, in 2006, a computer virus spread to ATC systems forcing the FAA to shut down a portion of its systems in Alaska.[84] A subsequent report from the Office of the Inspector General (OIG) discussed that it was a matter of “when, not if” a cyberattack could seriously harm ATC operations.[85]

The 2009 warning from OIG has similarities to some GAO reports referencing ATC/ATM cybersecurity. A 2015 GAO report stated that the FAA needed a “. . . more comprehensive approach to address cybersecurity . . .” in the transition to NextGen.[86] Another report specifically highlighted the cybersecurity challenges of protecting ATC systems that, unless addressed, would place *“*. . . the safe and uninterrupted operation of the nation’s air traffic control system at increased and unnecessary risk.”[87]

The recurring themes in these reports, such as authentication, encryption, auditing, monitoring, etc., closely mirror the challenges facing any other large complex organization attempting to secure its information architecture. The GAO highlighted that the transition to IP based services through SWIM increased the risk of compromise due to the mix of old and new technologies and potential weak points in the network.

ICAO started work on SWIM around 2005 and describes it as a “loosely coupled environment . . . where services are provided and consumed by a number of entities.”[88] This effectively makes SWIM an aviation industry intranet where information can be shared as easily between entities in the same region as with those across the world. Its rollout will

80 “ACAS Guide: Airborne Collision Avoidance Systems (Incorporating TCAS II Versions 7.0 & 7.1 and Introduction to ACAS X),” Eurocontrol, May 2016, https://www.eurocontrol.int/sites/default/files/content/documents/nm/safety/ACAS/safety-acas-II-guide.pdf.

81 Mykel J. Kochenderfer, Jessica E. Holland, and James P. Chryssanthacopoulos, “Next-Generation Airborne Collision Avoidance System,” *Lincoln Laboratory Journal* 19 (1), 2012, https://ll.mit.edu/publications/journal/pdf/vol19_no1/19_1_1_Kochenderfer.pdf.

82 Joe Greenwood, “Crash All The Flying Things! – Exploiting and Defending Aircraft Collision Avoidance,” Security Tube, 2015, http://www.securitytube.net/video/13668.

83 Strohmeier, “Security in Next Generation ATC Networks.”

84 Elinor Mills, “Hackers Broke into FAA Air Traffic Control Systems,” CNET, May 8, 2009, https://www.cnet.com/au/news/report-hackers-broke-into-faa-air-traffic-control-systems/.

85 Ibid.

86 “FAA Needs a More Comprehensive Approach.”

87 “FAA Needs to Address Weaknesses in ATC Systems.”

88 “Manual On System Wide Information Management (SWIM) Concept,” ICAO, https://www.icao.int/airnavigation/IMP/Documents/SWIM%20Concept%20V2%20Draft%20with%20DISCLAIMER.pdf.

develop over blocks of five years beginning 2018 with increased network connectivity through each block.

As discussed by ICAO, "Starting from Block 2 [2023] and into Block 3, the aircraft should be fully connected to the network as a SWIM access point, enabling full participation in collaborative ATM processes with access to voluminous dynamic data."[89] It is noted that, as a developing program, there are many details that still need to be worked out on how aircraft cockpits will be securely connected to a global intranet such as SWIM. The security layers between the aircraft and potential adversaries will have to be extremely robust and highly resilient considering the criticality of compromise. Developing such a system will be complex and require input from multiple stakeholders with various perspectives. The ICAO Secretariat has declared that the overarching cybersecurity requirements of SWIM be drawn from:

- Annex 17, ICAO Aviation Security Manual (ICAO Doc 8973) and
- ATM Security Manual, Part A: Protection of ATM System Infrastructure (ICAO Doc 9985).[90]

Additionally, cybersecurity measures at a (SWIM) network and application level "should form the common foundation enabling each State to implement its national measures," with each state establishing "its own National Security Programme."[91] The work to mature SWIM governance and focus on cybersecurity is ongoing and may take a while, particularly since, as the International Coordinating Council of Aerospace Industries Associations pointed out, "There is not a globally accepted definition of SWIM and a clear guideline for its implementation."[92]

In the United States, for the past ten years, the FAA has been moving expeditiously on SWIM rollout and cybersecurity. This has included the development of four security gateways "providing accessibility between internal applications to external users" and providing "a physical separation 'air-gap' between the FAA operational network and all external users."[93] Additionally, the FAA has explored the identity access management needs around the rollout of SWIM in coordination with Eurocontrol.[94]

ICAO additionally set up the INNOVA Task Force in January 17, 2017, to better understand the governance and cybersecurity around a global SWIM architecture and its cybersecurity by exploring topics such as establishing standards as well as practices for IP addressing, IPv6, and public key infrastructure. Other ongoing research explores, for example, the development of use cases for aviation domain name system networks and the prototyping (hardware and software) of an airborne IP Suite router, which is being led by 'The Clean Sky 2' project funded by the European commission.[95]

SWIM will offer a great deal of useful functions to global ATM services, but issues around complexity, governance, and varied maturity levels appear unresolved and will make securing SWIM a considerable challenge. A number of contributors expressed unease about SWIM as a system with global access points, bringing acute concern of threat propagation (worm type attacks) or adversaries pivoting across systems. With increasing IP connectivity between multiple systems (ground based and airborne) over wide geographical areas, the potential for such attacks and failures must be considered and mitigated against. Fallback options will be in place to help prevent safety errors, but it must be remembered that this comes at the cost of capacity.

Capacity – The Challenge with Fallback Systems

A single compromise of one of the systems mentioned in previous sections is likely to cause inconvenience and a degree of service disruption. Through the very nature of system evolution, many of the backup systems for all of these discussed NextGen and similar worldwide systems have a reduced capacity. In the event of an incident that

89 Ibid.

90 Ibid.

91 Ibid.

92 "Observations and Considerations for the Implementation of SWIM," The First Meeting of System Wide Information Management Task Force (SWIM TF/1), ICCAIA, May 10-12, 2017, https://www.icao.int/APAC/Meetings/2017%20SWIMTF1/IP13_ICCAIA%20Observations%20and%20Considerations%20for%20the%20Implementation%20of%20SWIM_v2.pdf.

93 "FAA: 10 Years of SWIM Experience Introductory Best Practices and Lessons Learned Brief Overview of the SWIM Program," The First Meeting of System Wide Information Management Task Force (SWIM TF/1), FAA, May 10-12, 2017, https://www.icao.int/APAC/Meetings/2017%20SWIMTF1/WP06_FAA-Brief%20overview%20of%20the%20SWIM%20Program%20-2017-0508.pdf.

94 "Identity Access Management," The First Meeting of System Wide Information Management Task Force (SWIM TF/1), FAA, May 10-12, 2017, https://www.icao.int/APAC/Meetings/2017%20SWIMTF1/WP06_FAA-SWIM%20SECURITY%20CAPABILITIES%20and%20IAM.pdf.

95 "Minutes of the Twenty-Second SC-223 Plenary Meeting 'Internet Protocol Suite (IPS) and AeroMACS,'" RTCA, May 23, 2017, https://www.rtca.org/sites/default/files/sc-223_may_2017_minutes.pdf.

Air Traffic Controllers in Rungis, France. *Photo credit:* Bernard Rousseau, THALES.

causes reversion to legacy systems, controllers have to revert to legacy separation distances and may have to reduce airport landing and departure rates.

The greater the incident's impact or number of affected systems, the more capacity will be reduced. When operating at full capacity on NextGen type systems, cascading to fallback systems will create a host of challenges. Therefore, the dismissal of concerns about NextGen vulnerabilities because of the availability of backup legacy systems may miss that ATM is a complex system sensitive to impacts against capacity and throughput.

Future ATM systems are truly groundbreaking for the industry and have numerous benefits for the aviation industry and the passengers it serves. When delivered, it will bring global capacity, predictability, and reliability. But it must be recognized that when initially conceptualized, remote attackers exploiting insecure links was almost unthinkable. As a result, most of its underlying architecture has been designed and baked in without adversaries in mind. Therefore, as the industry moves forward, it is very much with a focus on mitigating and protecting what is already insecure.

Airports

SECTION TAKEAWAYS

- 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.
- Appropriate cybersecurity of physical security systems at airports is critical.
- Successful cyberattacks against public-facing information systems at airports may pose little safety risk, yet are likely to negatively affect public confidence and trust.

Enabling and keeping air operations safe and efficient is a task that starts on the ground. Successfully moving large quantities of people and cargo in and out of an airport while delivering all the supporting services is no small feat. In addition to maintaining smooth operations twenty-four hours a day, 365 days a year, the safety and security team must ensure that airport infrastructure, passengers, and aircraft are protected against a multitude of threats. As connected technologies are increasingly transforming these ground services, it is critical to understand what the future might look like and the challenges this might bring.

The Current Situation

The main objective for airport management and security is to safely dispatch and receive aircraft, passengers, baggage, and cargo. As such, the airport is the focal point for a large proportion of aviation operations and on the front lines of securing against adversaries—a narrative that came up repeatedly during the research.

The importance of improving cybersecurity at airports should therefore be obvious. Yet as a contributor commented, airports are a federated management service, which represents numerous companies and organizations under different risk owners and governance structures, all contributing to security and service delivery. Therefore, airport cybersecurity must be considered from the perspective of securing multiple systems being operated by multiple providers who can either contribute to shared awareness and resilience or be the critical weakness.

Airports – A Connected Target

With the concerted effort that terrorists put into compromising physical security, securing the physical domain has inevitably been a high priority. As airport monitoring and services are increasingly connected, there may be opportunities for adversaries to facilitate physical domain attacks by compromising the virtual. So far, cyberattacks against airports have had a disruptive effect on operations or unsettled passengers. Although they generally receive less publicity, instances of cyberattacks on airports include

- the teen that shut down an airport's radio and telephone systems for six hours;[96]
- the 2013 discovery of an APT targeting seventy-five US airports, successfully compromising two of them;[97]
- disrupted flight plans leading to 1,400 grounded LOT Polish airline passengers in an attack that was subsequently traced back to a breach of airline computer systems at Warsaw Chopin airport;[98]
- attacks on Vietnam's two largest airports and its flag carrier where information screens and

96 Festa, "DOJ Charges Youth in Hack Attacks."

97 Andrew Blake, "Cyberattack Claims Multiple Airports in Vietnam," *The Washington Times*, July 29, 2016, http://www.washingtontimes.com/news/2016/jul/29/cyberattack-claims-multiple-airports-vietnam-airli/.

98 Rene Marsh, "Hackers Successfully Ground 1,400 Passengers," CNN, June 22, 2015, http://edition.cnn.com/2015/06/22/politics/lot-polish-airlines-hackers-ground-planes/index.html.

sound systems (as well as the airline website) were hijacked.[99]

Many of the above attacks were seemingly motivated to cause disruption for ideological, financial, or mischievous purposes. The now networked physical security devices at airports is an attack surface that has yet to be exploited.

The research community is becoming increasingly interested in airport security infrastructure. As an example, in 2014, researchers investigated the cybersecurity of airport security devices. Researchers claimed they were able to control or mask the images that operators saw on an investigated baggage scanner and they were able to modify the detection capabilities of drugs or explosives scanners.[100] Although the Transportation Security Administration (TSA) dismissed the researcher claims by saying that their "software cannot be hacked or fooled," the blending of network connectivity with critical security equipment will always raise concerns about how to protect it.[101]

. . . [T]he blending of network connectivity with critical security equipment will always raise concerns about how to protect it.

OIG produced a redacted report on the audited challenges in TSA's Security Technology Integrated Program (STIP).[102] The report highlighted that STIP, which enables remote networked management of passenger and baggage screening devices, had several security control deficiencies including not scanning STIP servers for technical vulnerabilities, allowing non-DHS employees access to STIP server rooms, not including STIP servers in wider information security plans, and not establishing interconnection security agreements between STIP and non-DHS baggage handling systems.[103] It was also revealed that many of these security devices had not been designated as IT equipment and therefore not treated as such with respect to their security.[104]

The main observation that can be made from the OIG audit is that, as networked technology and IoT are deployed as a critical underpinning layer of maintaining security, efforts to secure that technology must happen simultaneously. This observation is equally applicable for airports as they seek to embed IoT across their estate. Identifying it and protecting it will be essential, since not doing so will risk creating critical weakness.

Taking It Forward

Airports face challenges similar to those of many large safety critical organizations with IoT devices and safety critical systems, such as oil and gas installations, except that the federated nature of airports creates additional complexity. Some airports have awoken to the cyber threat and are putting in the people, processes, and technology to better protect themselves. As this matures, having an airport-wide cybersecurity strategy led by senior management will become more and more commonplace. Such a structure will also have to work with other airport stakeholders that are likely to have similar structures. The strength of airport cybersecurity will not be dictated by the individual quality of one of these structures, but by how well all of them collaborate.

There has already been discussion of airport Internet Sharing and Analysis Centers (ISAC) that can help form a united front across all airport operators to promote collaboration and sharing of cybersecurity information. It remains to be seen if such a formal organizational ISAC-type structure is required, but sharing and collaborating across the airport ecosystem will be essential. There are multiple ways that such collaboration can be leveraged. Knowledge management, vulnerabilities, and threats can all be used to improve preparedness at a strategic level. But work done together to prepare or prevent must also be matched by efforts to collaboratively respond in the event of an attack.

Security exercises in the physical domain have long since tested airport security measures, producing valuable lessons for stakeholders in how they might improve. Likewise, cybersecurity must also be tested

99 Aliya Sternstein, "Nation State-Sponsored Attackers Hacked Two Airports, Report Says," Nextgov, June 19, 2014, http://www.nextgov.com/cybersecurity/2014/06/nation-state-sponsored-attackers-hacked-two-airports-report-says/86812/.

100 Billy Rios and Terry McCorkle, "Pulling the Curtain on Airport Security," Blackhat, 2014, https://www.blackhat.com/docs/us-14/materials/us-14-Rios-Pulling-Back-The-Curtain-On-Airport-Security.pdf.

101 Ibid.

102 "IT Management Challenges Continue in TSA's Security Technology Integrated Program (Redacted)," Office of the Inspector General, May 9, 2016, https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-87-May16.pdf.

103 Ibid.

104 Ibid.

Passengers making their way through airport security. *Photo credit:* Wikimedia.

and exercised as airport stakeholders try to refine organizational aspects of airport cybersecurity. Exploring how all airport stakeholders can work together during a cyberattack permits a degree of verification of preparedness and reinforces the value of collaboration. The sophistication of the exercise scenarios will mature over time, but hopefully both physical security and cybersecurity exercises will be conducted together. Such scenarios will be as valuable as they are challenging.

Airport cybersecurity guides have already been written to shape these efforts, the FAA sponsored 'Guidebook on Best Practices for Airport Security,' the European Union Agency for Network and Information Security's 'Securing Smart Airports,' and the IATA 'Aviation Cybersecurity Toolkit,' all offer comprehensive advice on airport cybersecurity.[105] These guides broadly complement each other, showing that there is a degree of agreement on best practice that airports can implement as they go forward. As difficult as it is to secure the airports of today, the challenge will only grow more demanding with the complexity of additional connected devices, data, and people.

Singapore's Changi Airport is exploring many of these 'future airport' technologies and is currently working on:

- automation and robotics—to optimize scarce manpower resources and empower the airport workforce to operate at higher efficiency and productivity levels;
- data analytics and IoT—to provide opportunities to enable a more accurate and real-time perspective of airport operations;
- non-intrusive security technologies—to enhance the passenger experience and reduce the stress of undergoing security clearance, while strengthening safety and security standards; and

105 Randall J. Murphy, et al., *Guidebook on Best Practices for Airport Cyber security*, Transportation Research Board, FAA, 2015, doi:10.17226/22116; "Aviation Cyber Security Toolkit," IATA, July 2015, http://www.iata.org/publications/store/Pages/aviation-cyber-security-toolkit.aspx.

- smart infrastructure management—to create opportunities to leverage new technologies such as sensors, IoT, and smart controls to optimize infrastructure resources.[106]

The aviation industry, passenger, and cargo services could benefit considerably from these airport technologies, but comprehensive cybersecurity measures must underpin all of them. Such advances in technology may seem a long way off or irrelevant to many airports that are just starting to build their technology programs or understand and better manage their cyber risk. It must be remembered, however, that the strength of a cybersecurity program is not driven by the nature of its technology or the technology it is protecting, but rather by its people, processes, culture, creativity, leadership, and teamwork. Irrespective of technology, this is the work that can take place now to better prepare for the future and that is what will make the difference.

106 "Changi Airport Launches Living Lab to Create next Generation of Solutions for the Airport," Changi Airport Group, press release, January 5, 2017, http://www.changiairport.com/corporate/media-centre/newsroom.html#/pressreleases/changi-airport-launches-living-lab-to-create-next-generation-of-solutions-for-the-airport-1722894.

REMOTE TOWER SERVICES

An ATC Tower manages the zone around the airport, coordinating aircraft as they land, takeoff, and drive around the airport. Traditionally this operation would be conducted by a number of controllers sitting in a raised tower with full visibility and ground-to-air communications, but such a tower can be expensive in both infrastructure and personnel costs. This means that airports with limited aircraft movements may have no tower at all with aircraft procedurally deconflicting from each other as they operate in and around the airport.

As technology advances, the Remote Tower Services (RTS) concept is gaining more and more traction. In it, the manned tower is replaced by a number of cameras (visual and thermal), sensors, and radios that are all transmitted back to a remote virtual tower which may be hundreds of miles away. Here ATC controllers surrounded by high definition screens control the virtually presented but real aircraft.

For some airports, such as Jersey in the United Kingdom, this type of capability is seen as a robust backup in the event of having to evacuate the staffed real tower or in the event of failure.[1] But the predominant rollout of RTS was initially focused on giving small, remote regional airports with few aircraft movements, a functioning but remote tower. Now, as the concept becomes more established, ever larger airports are being converted or considered for RTS.

In the United Kingdom, City Airport in the heart of London has around 4.5 million passengers a year and is being converted to a RTS that will be operational in 2019.[2] Multiple fiber networks will transmit images and communications from London City Airport to a control room around 70 miles away.[3] When asked about the security aspects, the Chief Executive of London City Airport expressed confidence in the systems as being secure, safe, and "managed very well" with a spokesman declaring that the systems had been "stress-tested by IT security experts."[4]

As RTS becomes more commonplace with initiatives across Europe and the United States, greater focus on their ability to "increase the level of safety or increase the safety of flight operations" is to be expected.[5] In parallel to this focus must be a robust, comprehensive, and objective assessment of risk and best practices. RTS is a novel technology with novel challenges and risks. Collaborating on security will be essential to delivering safety critical services across all RTS suppliers, as compromise of one supplier will likely impact trust in the others.

1 "Jersey Airport Spends £1.3m on Air Traffic Control Back-up," Bailiwick Express, March 4, 2017, https://www.bailiwickexpress.com/jsy/news/ports-jersey-spend-13million-technical-advances/.

2 "London City Airport and NATS to Introduce the UK's First Digital Air Traffic Control Tower," NATS, press release, May 19, 2017, https://www.nats.aero/news/london-city-airport-and-nats-to-introduce-the-uks-first-digital-air-traffic-control-tower/.

3 Ibid.

4 Saphora Smith, "London City Airport to Build Remote Digital Air Traffic Control Tower," NBC News, May 19, 2017, https://www.nbcnews.com/business/travel/london-city-airport-build-remote-digital-air-traffic-control-tower-n761981.

5 "ECA Position Paper: Remote Tower Services," ECA, 2014, https://www.eurocockpit.be/sites/default/files/eca_position_paper_rts_14_1107_f.pdf.

Organizations with both a commercial stake in the success of RTS as well as safety responsibilities will have to carefully navigate a course between safety and security objectivity and technology promotion. For example, if US ATC services are privatized as proposed, it may be required to set safety standards as well as balance the commercial drivers.[6]

The introduction of internationally regulated minimum standards for RTS cybersecurity and safety will be essential. Nationally, cybersecurity standards for RTS are maturing, but international agreement may be some way off. As an example of the challenge this may bring up, concerns were raised by the European Cockpit Association of cross-national border RTS operations creating a potential market in selective shopping for the most lenient regulatory regimes.[7]

There are a lot of sound reasons to develop RTS. From the perspective of a backup service or providing service where previously there was none, it is clearly a step forward, but as a remote service that is reliant on technology and connectivity, there are also risks. Adversaries have consistently shown interest in disrupting airports and their services. It is a given that they will assess and test the security of RTS. Ensuring that their efforts are unsuccessful will require a robust and collaborative approach from all industry stakeholders and regulators.

6 21st Century AIRR Act, H.R. 2997, 115th Cong., 1st sess. (2017), http://docs.house.gov/billsthisweek/20170717/BILLS-115HR2997-RCP115-25.pdf.

7 "ECA Position Paper: RTS."

A Tale of Two Sectors: Aviation and Cybersecurity

SECTION TAKEAWAYS

- The aviation and cybersecurity fields each understand their own domains. As those domains increasingly overlap, the common goals of safety, resilience, and trust can be achieved sooner by working together.
- Preserving aviation's strengths relies on clear definitions of governance and accountability, and in recognition of shared responsibilities across the supply chain and operational environments.
- While the goals of cybersecurity and aviation safety are very similar, the SMS approach taken by the aviation industry appears superior in collectively learning through adversity than current cybersecurity methodologies.
- How to incorporate and enable cybersecurity aspects within air accident or incident investigations remains to be standardized and matured.

There is more to the challenge of protecting the interconnected aviation industry than just becoming more secure. As the aviation industry and the cybersecurity industry increasingly intertwine, it is important for them to learn about respective strengths and weaknesses. Both industries will need to develop a cultural understanding of each other to jointly learn, support, and strengthen their relationship as they go forward.

As the cybersecurity industry is increasingly involved with the aviation industry, it must remember that it plays a supporting role to an industry that is already mature in maintaining safety critical services. The aviation and cybersecurity industries both face difficult challenges, not least understanding the relationship between safety and security. It is important to get the best out of both industries in developing a technologically advanced and connected aviation industry. This section explores some of the nuances and differences between the industries and highlights potential strengths, areas for collaboration, and challenges.

Risk Management, Governance, and Accountability

The aviation industry is highly experienced in managing complex risk in a challenging environment. It has very clear governance and accountability structures and an embedded safety culture that ensures all personnel feel personal responsibility for managing risk and maintaining safe operations. Such a culture is demonstrably less clear-cut when it comes to information security risk and discussions abound about the pathway of responsibility and accountability.

The GAO review on FAA information security stated that "several entities within ATO [Air Traffic Organization] share responsibility for information security-related activities over air traffic control systems."[107] Managing cybersecurity through shared responsibility creates the possibility of a risky shift effect and challenges of not only understanding true risk but also overall accountability. It can also be difficult to hold a diverse working group or committee to account. The aviation industry is not alone in this challenge. Right Honorable Andrew Tyrie, Member of Parliament, Chairman of the UK

107 "Civil Support: DoD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber

Treasury Committee, highlighted that across the UK financial industry "the lines of responsibility and accountability for reducing cyber threats remain opaque" and that "a single point of responsibility for cyber risk in the financial services sector—with a direct line of accountability to a single official . . . is now required."[108]

The complex multiple suppliers and service relationships on both the aircraft and across the industry make it challenging to know who holds responsibility where. For example, understanding where responsibility sits—with either OEM, the airline, the Sat Comm provider, or the GSM provider—will be critical. As more providers bring more services and complex relationships and communications onto aircraft, airports, or alongside critical services, clear accountability for safety and security must be assured. An opaque multi-stakeholder committee will not be sufficient.

Fundamentally, with a connected, technologically advanced aviation industry, the SMS is still the primary method to manage safety. Irrespective of information security governance, if it intersects with safety critical systems, it is part of the SMS. The safety teams are focused on preventing accidents and the cybersecurity teams on preventing subversive malicious intent; both teams have differences and nuances in achieving their aims but must work toward a single vision. With connected technologies that require security to be interwoven with safety critical aviation services and platforms, the relationship between safety and security will have to be closer and more clearly defined than it has ever been.

Florian Guillermet, then Executive Director of the SESAR Joint Undertaking, asked, "Is security so different than safety and can we aim at a Safety *and* Security Management System?"[109] Evidence is building that such an objective may be key to a safe and secure aviation industry, but achieving it will require close collaboration between all stakeholders.

Preventing Failure

As a highly regulated, safety-focused industry, aviation is well-versed in predicting, mitigating, dealing with, and recovering from failure. This encompasses all aspects of people, processes, and technology. If an incident is prevented, personnel are encouraged to be open and honest about the situation that led up to the save and the findings are distributed to others so that they can learn from their peers. This positive, flight safety culture successfully uses aviation industry personnel as human sensors to constantly look out for safety issues, report them, fix them, and learn from others. The aviation industry is highly collaborative in how it shares detailed accident, incident, or near-miss data with the industry-wide aim of never suffering the same accident twice.

The aviation ecosystem must be prepared to investigate cybersecurity aspects to aviation accidents or incidents.

It is safe to say that the cybersecurity industry is struggling to achieve the same level of sharing and learning. As it moves forward with the aviation industry, it must work with the sharing culture that is already in place. Despite the clamor about sharing cybersecurity data, both industries need to demonstrate the value in sharing for the practice to improve. This value is highly apparent in the aviation industry because there is a sense of shared responsibility to reduce risk. A just culture, where honesty and openness is valued and protected in the event of human error or mistake, ensures that learning happens fast and widely for flight safety. The same principles must be applied to successfully collaborate on cyber safety and security.

In delivering safe and secure systems, the delivering organization must make a number of assessments about how safe or how secure their product or service is. The aviation industry's well-established principle of independent audits and assessment of such assumptions, on the whole, has been very effective, but accidents have occurred on several occasions when audits were not carried out or their independent nature had been compromised. As the aviation ecosystem looks to standardize how cyber safety can be assured, the value of independent audits is already understood in the aviation industry and may be a good starting point.

108 Andrew Tyrie, "Responsibility for Reducing Cyber Threats Remains Opaque," Commons Select Committee, UK Parliament, March 23, 2017, https://www.parliament.uk/business/committees/committees-a-z/commons-select/treasury-committee/news-parliament-2015/responsibility-for-financial-cyber-crime-16-17/.

109 Florian Guillermet, "Security by Design," in ICAO Cyber Summit, April 6, 2017, https://www.icao.int/Meetings/CYBER2017/Presentations/Summit%20Day%202%20-%206%20April%202017/Session%206%20-%20P05%20-%20Security%20By%20Design%20-%20SESAR%20JU%20-%20F.%20GUILLERMET.pdf.

Once an aircraft is certified, its weaknesses and limits may be known. For connected technologies, however, these weaknesses evolve over time. Therefore, ongoing regular independent audits of security are likely to be required. In the cybersecurity industry, the value of independent assessment is gaining more traction through things such as bug bounty programs, penetration tests, red teams, etc. Some aviation companies are already promoting such schemes—and those efforts should be applauded and supported. Still, aviation cybersecurity is not just a technical activity. Audits of technology must be augmented by exercises that incorporate the entire organizational hierarchy. This will help senior management check their own assumptions and better define the lines between safety and security.

Dealing with Failure

Despite efforts to make the aviation industry as safe as possible, accidents still happen. Despite efforts to make connected industries as secure as possible, critical compromises still occur. It is reasonable to assume that as the blending of aviation and technology moves forward, a cybersecurity incident will, at some stage, impact a critical aviation service despite the combined effort to secure and assure these systems. The aviation ecosystem must be prepared to investigate cybersecurity aspects to aviation accidents or incidents. Deliberating on investigation methods after the fact will be too late. Time will be of the essence for learning, adapting, and securing the entire global industry.

For aviation, the US National Transportation Safety Board (NTSB), the UK Air Accidents Investigation Branch (AAIB), and other similar organizations globally, provide independent investigation of aviation incidents or accidents. Although there have been discussions and calls for something similar in the cybersecurity industry, it does not yet exist.[110] As aircraft, ATM, and airports are increasingly interconnected, investigating the cybersecurity perspectives of an incident or accident will become a critical aspect of the investigatory role.

In the event of an accident, this investigatory role is carried out by the national organization with jurisdiction over the geographic area where the incident occurs. This could mean that to investigate an accident, a state may request software, data, network logs, and any other information considered relevant to the investigation. Very rarely is a cybersecurity incident investigated by a third, potentially international party. There is scope for a great deal of tension not just between the safety and security aspects of investigating accidents (separate investigations may be divisive) but also internationally, as policy is yet to be agreed upon or precedent set.

Since the challenge is novel, it is unclear what cyber investigation capabilities the NTSB/AAIB or similar investigatory teams have or need to be equipped with. If the cyber aspects of the investigation are delayed, confused, or obstructed it will only degrade wider stakeholder trust in both the aviation industry and the findings. Maintaining trust in the investigation will require parity of investigatory pace, breadth, and depth between the safety and cybersecurity aspects.

110 "Should a National Cyber Safety Board Be Created to Help Report on Breaches?" RSA Conference, February 27, 2014, https://www.rsaconference.com/events/us14/agenda/sessions/1089/should-a-national-cyber-safety-board-be-created-to.

Policy and Regulation

SECTION TAKEAWAYS

- While national and international policies and regulations are agreed and understood for safety and physical security, it is yet unclear how aviation cybersecurity can achieve the same maturity and clarity.
- ICAO is in a strong position to draw together the numerous global aviation cybersecurity initiatives and then bring coherence, leadership, and set standards.

It will take leadership and a structured vision to take the industry forward. The aviation industry has been demonstrably successful in becoming safe, but work is ongoing to understand how cybersecurity underpins this safety. This cyber safety challenge will not be an easy one for the industry or international and national policy leaders, but collaboratively tackling it is critical for getting ahead of adversaries as well as for understanding and subsequently mitigating the risks.

The aviation industry has developed a top-down approach to standards and conventions for safe and secure global operations where different operators and nations can work together; this means requirements are well understood and global and national governance is clear. Although in development, many international standards and conventions are not yet in place for aviation cybersecurity. This may delay attempts to develop and align national strategies, for example, the UK Civil Aviation Authority's strategy for aviation cyber regulation is to define its "responsibilities for cybersecurity under existing EU/UK/International Regulations." In Europe, the upcoming NIS Directive on security of network and information systems may help aviation organizations understand what is required of them, but it will take some time to mature. Within the NIS Directive, air transport appears fairly comprehensive in its requirements for air carriers, airport managing bodies, and [air] traffic management control operators.[111] Which operators are 'in scope' for the NIS Directive will need careful consideration as some airports with less than roughly ten million passengers a year may not be required to be compliant. This risks the exclusion of comparatively small operators and suppliers due to scale but not their potential impact.

It will take leadership and a structured vision to take the industry forward.

Additionally, on November 16, 2017, EASA produced the Bucharest Declaration on high-level efforts in civil aviation cybersecurity.[112] With a focus on "protecting the European aviation system against cyber threats," the Declaration proposed several objectives such as coordination at a European level, international collaboration, information sharing, risk assessments, increasing awareness, and research. There was also a desire for regulations to be internationally harmonized, highlighting that despite being a supranational body, the challenges need an even wider, holistic approach.[113]

US efforts to promote aviation cybersecurity include the previously discussed 'Cyber Air Act,' which, along with clearer DHS guidelines for securing critical transport infrastructure, has shown a great deal of proactivity and action. These advances may be on the back of some searching GAO reports on

111 "Directive (EU) 2016/1148 of the European Parliament and of the Council," European Parliament, July, 19, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

112 "High Level Meeting: Cybersecurity in Civil Aviation Bucharest Declaration," EASA, November 8-9 2016, https://www.easa.europa.eu/system/files/dfu/Declaration%20from%20HLM%20Cybersecurity%20Romania%20-%208-9%20Nov%202016.pdf.

113 Ibid.

such topics as GPS, ATM, and ATC vulnerabilities, but they show that awareness of the cybersecurity challenges and, more importantly, a desire to find solutions is increasingly at the forefront of thinking at senior levels.

Such national and regional endeavors to improve aviation cybersecurity will foster diversity of dialogue. But as states and regions work to gain perspective on the challenge and develop a way forward, it is critical to preserve the international alignment that has been so successful for the aviation industry.

The ICAO aims to "develop the principles and techniques of international air navigation and to foster the planning and development of international air transport" to "insure the safe and orderly growth of international civil aviation throughout the world."[114] With these aims, the role of ICAO in setting global standards for aviation cybersecurity cannot be in question; how to drive it forward, however, is slightly more complex. To do this, ICAO must find a policy vehicle that is aligned with the challenge. The previously mentioned aviation cybersecurity framework that it is developing with partner nations will greatly help promote standards, but there may be an additional vehicle to globally set standards.

The Chicago Convention was signed in 1947 "in order that international civil aviation may be developed in a safe and orderly manner."[115] Updated to reflect the evolution of the industry and technology (Article 8, for example, highlights special authorizations required for pilotless aircraft), the Convention focuses on how to keep order and uniformity across a global industry so that collaboration and growth is promoted. This is highlighted in Article 37 where states undertake "to collaborate in securing the highest practicable degree of uniformity in regulations, standards, procedures, and organization."[116] If the Chicago Convention is the document that sets safe global standards for aviation security, Annex 17 is of greatest interest to cybersecurity.

Annex 17 of the Convention focuses on security and maintaining safety of flight by preventing "unlawful interference" of aircraft.[117] The Annex's current concern is with physical interference, but as explored within this report, potential unlawful interference through cyber means is now a reality. Incorporation of cyber perspectives into Annex 17 could be done with many parallels to the current physical focus, not least by setting out the parity of unlawful interference through cyber means.

Therefore, if a document were to drive and set global standards for aviation cybersecurity, Annex 17 of the Chicago Convention could be it. Amended to reflect the reality of an interconnected aviation industry, it would not only promote coherency in developing global aviation cybersecurity standards between nations, it would also promote dialogue and collaboration between disparate stakeholder groups—a key requirement for future success.

114 "Strategy: Guiding International Civil Aviation into the 21st Century," ICAO, February 7, 1997, https://www.icao.int/Documents/secretary-general/rpereira/strategy.pdf.

115 "Convention on International Civil Aviation," ICAO, 9th Edition, 2006, https://www.icao.int/publications/Documents/7300_cons.pdf.

116 Ibid.

117 Ibid.

The Foundations of Aviation Cyber Safety and Security

"If you think that technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

Bruce Schneier [118]

The previous sections explored aviation cybersecurity from the perspective of aircraft, ATM, and airports, comparing the potential strengths and challenges of delivering cyber safety and security. This section will condense the previous sections into what can be considered the key foundational pillars of aviation cyber safety and security. As has been discussed, aviation cybersecurity is a complex, multi-stakeholder activity that has an implicit requirement to maintain safe aviation operations in the face of adversary motivations.

With multiple perspectives and stakeholders, having a coherency and clarity of vision will be essential as the aviation industry becomes further interconnected. This report suggests the following vision:

"A safe and prosperous aviation industry with resilient trust and systems."

To achieve this vision, a number of themes repeatedly arose during the report which were seen as foundational to addressing the aviation cybersecurity challenge. These themes have been developed into what may be considered the foundational elements of the vision and are highlighted below.

Coherent Systems Thinking, Governance, and Accountability

The aviation industry is a complex, international ballet run by thousands of people using a multitude of different systems of differing maturities. This system of systems was not designed with potential adversaries in mind and has grown organically out of a focus on safety, efficiency, margins, and managing disparate systems. Previously discussed IT outages have demonstrated that this system of systems is sensitive to disruptions.

As the report has already explored, the complexity and interdependence of aircraft, ATM, and airports at organizational, national, and global levels is considerable. It is easy to see how numerous weak links in the chain can be developed.

In an interconnected system of interdependent systems, weak links can sit unnoticed and risk disproportionate effect. Everything learned from cybersecurity indicates that attackers will target weak links to achieve their objectives. Examples, such as the compromised high-volume air conditioning unit that lead to the Target breach or the fish tank that compromised the casino, demonstrate that a system can only be as strong as its weakest link.[119] In the drive to improve aviation cybersecurity, finding and securing the

118 Bruce Schneier, Secrets and Lies: Digital Security in a Networked World (Indianapolis: John Wiley & Sons, 2000).

119 Mark Hosenball, "Target Vendor Says Hackers Breached Data Link Used for Billing," *Reuters*, February 6, 2014, https://www.reuters.com/article/target-breach-vendor-idUSL2N0LB1TM20140206; Lee Mathews, "Criminals Hacked A Fish

weak links in the system, whether in operations or deep in the supply chain, is not only an essential requirement but also a critical test of governance and accountability.

It will take leadership from the top down to improve governance and accountability in the global aviation ecosystem no matter where the weak links are. This reinforces the work ICAO is doing with national regulators to decide how the aviation industry should deal with cyber risks and then cascading best practices and processes out to all stakeholders. This activity will not just improve the management of cybersecurity risk, it will also likely considerably clarify and simplify the legislative burden for aviation industry stakeholders.

Resilient Systems

Aircraft systems are designed to safely degrade in the event of failure. Against capable adversaries "even with correct implementation of all the necessary perimeter-based security, and continuous monitoring to ensure that patches are applied and vulnerabilities are closed, advanced adversaries will still breach the IT infrastructure."[120] This assumption of future breach and potential failure has resulted in a greater focus to continue to deliver safe operations and business processes, regardless of what the adversary is attempting to achieve or what they have compromised.

The Community Emergency Response Team (CERT) Risk Management Model defines operational resilience as "the emergent property of an organization that can continue to carry out its mission in the presence of operational stress and disruption that does not exceed its operational limit."[121] From this definition, it is possible to distinguish the nuance between cybersecurity, attempting to prevent compromise, and cyber resilience, safely working through stress and disruption caused by compromise. Both are equally important and complimentary. Striving for both results in resilient systems engineering practices and a resilient culture embedded within personnel.

The importance of cyber resilience in aviation was highlighted in a working paper presented to the 39th ICAO assembly that addressed cyber resilience. After acknowledging that the potential for cyber incidents has increased over the years, it called for ICAO to "develop globally coherent cyber resilience approaches for the aviation system."[122] Such a global approach will go a considerable way in balancing the requirement to be secure with the reality of needing to be resilient.

Resilient Trust

The importance of stakeholder trust is at the forefront of the aviation cybersecurity challenge. The birth of commercial aviation was not easy and had false starts until there was widespread acceptance of aviation as a method of travel. James G. Woolley, former Vice President of Western Air Express, possibly the first successful airline, spoke of how transportation by airplane advanced from a "wildly speculative, much mistrusted, extremely dubious venture to recognition as an established industry commanding the confidence and respect of the entire Nation."[123] The aviation industry went from being "much mistrusted" to building a foundation of trust globally. But trust is hard-earned and easily lost. An absolute focus on safety has so far managed to nurture and preserve trust in the industry even though the power of headlines in an 'always on' society is such that bad news travels fast and trust can be eroded quickly.

The aviation ecosystem must consider the challenge of building trust in tandem with cybersecurity challenges. If claims are made against an aviation system or aircraft, proving trustworthiness to all stakeholders may be difficult. Arguably, if it takes weeks and millions of dollars to prove or regain trust, such as in the Chris Roberts case, then there is a considerable way for the industry to go. Being able to investigate potential issues quickly and, more importantly, demonstrate potential impacts and mitigations will be an essential skill for the aviation industry in the future. This will require moving away from security through obscurity to a place where the industry can successfully demonstrate why stakeholders and passengers should and can trust them.

Irrespective of how good the security of safety critical software is, if adversaries can erode trust, it gives them the ability to control passenger experience, perspective, and confidence. If passengers or regulators are given enough ground

Tank To Steal Data From A Casino," *Forbes*, July 27, 2017, https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/#40d73acd32b9.

120 Deb Bodeau and Richard Graubart, "Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls," Mitre, 2013, https://www.mitre.org/sites/default/files/publications/13-4047.pdf.

121 "CERT ® Resilience Management Model, Version 1.2 Glossary of Terms," Carnegie Mellon University, http://www.cert.org/resilience/.

122 "Cyber Resilience in Civil Aviation," ICAO, July 26, 2016, https://www.icao.int/Meetings/a39/Documents/WP/wp_099_en.pdf.

123 James G. Woolley and Earl W. Hill, *Airplane Transportation* (Hollywood: Hartwell, 1929).

Photo credit: William Perugini.

to question an aircraft, system, or airport for any reason, the operator has to counter that perception and rebuild trust. The longer this takes, the less credibility the operator will have in the eyes of the stakeholder.

Secured Human Decision-Making

Human operators are the last link on the safety chain and their ability to make and execute timely, well-informed and safe decisions is a cornerstone of aviation. Protecting this ability from the risk of data integrity attacks and adversary subversion is essential.

The technology to help humans make safe decisions at the right time is in place across the aviation industry. As long as they are presented with correct, timely information, people will follow their training and act accordingly. If that information is incorrect or coming at them too fast or too late, however, decision-making becomes difficult and mistakes are more likely. If the information presented becomes confusing or overwhelming for aircrew, ATC, etc., it can degrade SA and compromise the ability to conduct their primary role. For those in supporting roles, such as engineers and schedulers, the challenges of maintaining focus and accuracy are no less important; degradation of capability, increased workload, and additional distractions can all lead to critical errors.

Human error or technical failure is inevitable, but all aviation systems are designed to help a human operator recognize and deal with an accident or incident before it impacts safety. Therefore, when securing technology, there must also be a focus on protecting the integrity of the data that operators are presented with so they are able to make safe decisions.

Now that operators may have to make decisions during potential adversary interference or subversion, the aviation industry must consider to what extent operators, such as aircrew or air traffic controllers, should become involved in their own cybersecurity or remain focused on their primary role. Finding the correct cyber resilience balance between good system design and relying on the end user is an essential debate. Notwithstanding, aviation operators are well-versed in dealing with failure, mechanical or otherwise. Learning how to react to cyberattacks with effects ranging from denial to subversion will be a different challenge

requiring the training to match. The importance of such an initiative has already been raised by the International Federation of Air Line Pilots' Associations, which called for training to help pilots recognize cyberattacks.[124]

Shared Perspective and Culture

The importance of collaboration cannot be underestimated. Even beyond sharing knowledge and perspectives, there is great potential for cultural exchange between the aviation and cybersecurity industries.

Having already explored the aviation industry as a system of systems, vulnerabilities are likely to be mirrored across multiple regions, nations, or service providers. Comprehensive and timely information sharing will minimize systemic risk, for once a cyber vulnerability is discovered, it becomes a race to patch it no matter where it is deployed.

Sharing sensitive information regarding vulnerabilities and threats is not an easy task. The growth of ISACs relevant to the aviation industry is taking place both in the United States and in Europe. They enable participating organizations to receive knowledge about vulnerabilities and intelligence about threats in a manner that helps them better manage cybersecurity risk.

For such organizations, sourcing and developing valuable insight and distributing it across a trusted collective are key drivers, but a degree of stratified threat and vulnerability sharing must be accepted because levels of trust vary. Research is ongoing as to how the development of trust could be accelerated, but fundamentally it takes investment in time, effort, and increasing collaboration. For example, the Aviation-Information Sharing and Analysis Center (A-ISAC) is looking to the collaborative work between the National Aeronautics and Space Administration and Russia as an example of how nations can work together on complex, technological projects that have exacting safety requirements.

The A-ISAC has already been involved in incidents where its ability to quickly share knowledge has successfully mitigated risk across multiple international stakeholders. The value of such collaborative work extends past knowledge about vulnerabilities or threats to those involved. The A-ISAC is also a focal point for best practice and a cybersecurity force multiplier. The newly set up European Center for Cybersecurity in Aviation has similar goals to the A-ISAC with links back into the EU CERT.[125] These organizations are aiming to take collaboration to a level where valuable sharing can occur and learning can take place across multiple stakeholders irrespective of their cultural outlooks.

The aviation industry has a strong culture of safety embedded into all of its activities. As it intertwines with the IT industry, a key requirement will be to understand and overcome the cultural differences between the groups. One contributor described this as a large challenge that would require global reform. Developing a shared culture in which both groups synergize and view the challenges and potential solutions together will require cross-disciplinary learning and sharing of cultural approaches. The benefits of such a shared outlook and vision will be increased awareness of risk and robust resilience.

124 "Cyber Threats," IFALPA, December 6, 2016, http://www.ifalpa.org/downloads/Level1/IFALPA%20Position%20Papers%20&%20Statements/Security/16POS08%20-%20Cyber%20Threats.pdf.

125 "Implementation of a European Centre for Cyber Security in Aviation (ECCSA)," EASA, April 4, 2017, https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa#group-easa-related-content.

Suggested Next Actions

Improving aviation cybersecurity is a journey and not an end-state; therefore, the early steps are important, especially when addressing a challenge of considerable scale and complexity. This section lays out considered and specific recommended next steps for all stakeholders.

Next Actions for All Stakeholders

Reinforce Leadership and Standardization (Globally, Nationally, Regionally, etc.)

Challenge – The rapid incorporation and development of connected technologies within the aviation industry is only outpaced by the development of adversary capability. This has resulted in individual, organizational, and national efforts to manage and regulate in the face of the challenge.

Action – As the most senior aviation body addressing the challenge of aviation cybersecurity, the ICAO should provide recommendations to address the challenge and also clear requirements for the governance and accountability of cyber safety and cyber risk across the global aviation landscape. These considerations should be normalized alongside other ICAO regulations safeguarding against unlawful interference, such as Annex 17 to the Chicago Convention.

Define a Common Understanding of Aviation Cyber Safety and Security

Challenge – The governance and accountability of maintaining secure systems is primarily seen as a security role. How that translates to risk ownership and accountability in complex safety critical systems (with multiple suppliers) across the aviation industry is a challenge. Any confusion of accountability between safety responsibilities and security responsibilities is likely to obfuscate knowledge of the true safety risk.

Action – The aviation industry must ensure that the governance and accountability of cyber safety and cybersecurity is well understood, defined, robust, and fully incorporated into existing SMS. This must be done in a way that strengthens, not weakens, the well-established and effective SMS in place across the aviation industry. The more that this approach is globally standardized, the greater understanding of comparative true risk across the aviation industry will be.

Reevaluate, Develop, and Use Robust Threat Models

Challenge – The aviation industry has the unenviable security challenge of long hardware life combined with a long software patch cycle and a rapidly evolving threat landscape. When threats are being assessed to inform risk models, the difficulty is how much capability or motivation should be assigned to potential adversaries.

Action – Aviation cyber threat models must better encompass and predict adversary capability, motivation, and evolution throughout the entire lifecycle of the product or system. This activity will require collaboration across multiple stakeholders, be they government, aviation industry, or independent researchers.

Develop and Communicate Coherent Messaging on Cybersecurity Risk to Stakeholders

Challenge – There is not a coherent aviation industry position on the cybersecurity risk it faces. Some stakeholders still declare that systems are impervious to attack. In the event of a successful attack, it may be difficult to recover from the shift in stakeholder perception and loss of trust.

Action – The aviation industry must have clear, realistic, and coherent messaging about cybersecurity risks and the efforts to mitigate them. This will require bringing together stakeholders and generating a shared responsibility for solving problems rather than attempting to defend precarious positions.

Find Ways to Develop Trust with Non-Technical Audiences

Challenge – Years of safety improvements means that, to a large degree, stakeholders currently trust the aviation industry. The challenge of generating trust around cyber resilience is that much of the audience is non-technical. Physical security and safety measures are often visible and tangible, making it easier for stakeholders to understand and develop trust in them. The technical complexity of cybersecurity means that developing, communicating, and protecting trust will be more difficult.

Action – The aviation industry must find ways to build trust across largely non-technical passengers and stakeholders with respect to cybersecurity. This trust must be founded on the reality of cyber resilience and backed up with demonstrable measures. The more that such trust can be communicated and shown, the less impact cyber incidents or claims may have.

Improve Agility in Security Updates

Challenge – Installing hardware and software security updates within aviation safety critical systems are a lengthy process. As the aviation industry increases its connectivity, it is reasonable to assume vulnerabilities will be discovered and any attempt to obscure them is not a valid strategy. Other industries that have embraced connected technologies have discovered that once a vulnerability is discovered, patching quickly and efficiently to mitigate the risk is essential to preventing service and safety impacts.

Actions – Develop and implement aviation industry best practices for greater agility in security updates for both hardware and software. This should incorporate methodologies to both accelerate patch cycles (including secure rollouts) and develop in place mitigations to cover the vulnerability gap. Additional consideration should be given to how modification of certification policies and system design can assist the process.

Design Systems and Processes to Capture Cybersecurity-Relevant Data

Challenge – There is currently very little visibility, metrics, or logging of many interconnected aviation systems, making it a challenge to observe and assess Indicators of Compromise (IoC), let alone to remediate or secure. As many connected industries have discovered, prevention is ideal but detection is a must. Poor visibility of critical data or little collaboration on findings will make it extremely difficult to understand the scale of the cybersecurity challenge for the aviation industry.

Action – No matter the complexity of the system, the aviation industry needs to develop data capture abilities to detect adversary activity (IoC) in hardware and systems, be they operational or in the supply chain. The independence and rigor of post-crash management investigation must also be considered, permitting the investigation of potential cybersecurity aspects of any incident or accident.

Train for Safety Across Multiple Disciplines

Challenge – Aviation personnel, well-versed and trained to conduct safe operations, are likely to have to operate through disruptive cyber adversary actions. They are currently not trained to spot, assess, or appropriately react to such a situation, which greatly increases the potential impact of any adversary action. Likewise, cybersecurity personnel may not be trained to understand the nuances of aviation operations.

Action – The aviation industry must develop appropriate methodologies and training across multiple disciplines to equip all personnel with the skills to recognize adversary activity and maintain safe operations. In parallel, cyber incident response personnel must be trained in how best to support safe aviation operations in what are likely to be time-critical situations. This training may be especially valuable if observed lessons can be quickly fed back into the wider aviation ecosystem.

Incorporate Cyber Perspectives into Accident and Incident Investigations

Challenge – Aviation accidents and incidents are thoroughly and objectively investigated, often by national bodies. These investigations focus on recreating events in order to discern a root cause, so that the rest of the industry can avoid the same occurrence. How to incorporate cybersecurity aspects into such investigations—or if the necessary data is even available—is unknown.

Action – Investigate and propose best practice to enable appropriate investigation of cybersecurity aspects of aviation incidents and accidents. This should not only focus on organizational structures, authorities and technologies, but also on what may be required in aviation system design to permit timely and forensically sound investigations.

Conclusion

Governments, international bodies, and investors know the considerable value that a globally resilient and prosperous aviation industry brings, such as underpinning strong national growth, tourism, and manufacturing. Historically, low accident rates have bolstered trust and profitability, but this does not equate to resilience. In the aviation industry, an accident or attack can erode trust quickly, but even attacks on non-critical systems can degrade stakeholder trust and perceptions.

There may also be a gap in perceptions of potential adversary intent, capability, and subsequent risk facing the aviation industry; some stakeholders perceive little risk while others perceive considerable risk. Understanding and bringing these stakeholders together will be an essential aspect of holistically moving forward together. This will require clear dialogue and non-partisan collaborative effort on behalf of the stakeholders because the challenge has both complexity and depth; no one group holds all the answers. Now is the time for collaboration and action, not circular discussions.

Making aviation systems resilient against cyber adversaries stretches from concept through design, assurance, supply, build, delivery, and operations. With a shifting and evolving threat landscape that is growing as fast as the potential attack surface, managing risk and looking far enough ahead is a complex, multi-stakeholder challenge. In the key areas explored by this report, technological innovation was continually apparent, but innovation in risk perception was harder to find.

Aircraft, be they airliners, UAS, or helicopters, must now be considered as nodes on multiple networks, whether they are airborne or not. Multiple claims of opportunity and vulnerability must be met with more than dismissal. If any such claims subsequently become realized in any form, echoes of any dismissal will lead to potential loss of credibility and trust. It will take consideration and incorporation of multiple stakeholder perceptions to reduce the risk of adversaries seeing something the industry has not. In a complex, interdependent system, blind spots exist. Credit and support must be given to those wanting to shine a light into them.

To manage airspace in a connected world, there is much that technology can offer. Increasing efficiency and traffic density while reducing margins will permit the aviation industry to satisfy future demand. The technological foundation of this industry was conceived, designed, and agreed upon, but, in a period where adversaries with capabilities such as SDR and GPS jammers were not predicted. Therefore, system confidentiality, integrity, and availability requirements were not factored into development, and only considered after the fact. Even if backup systems are available, they have reduced capacity and capability. Targeted disruptive effects at a busy period will have significant impacts.

In a complex, interdependent system, blind spots exist; credit and support must be given to those wanting to shine a light into them.

Airports are a key focal point for multiple industry stakeholders and adversaries. Maintaining safety and security remains critical. To permit higher passenger numbers, increasing the use of technology to screen and assure passengers and baggage are but one example of both risk and opportunity. Multiple stakeholders are innovating and connecting services in what is a federated structure with multiple perspectives of risk. Getting them to collaborate and develop a shared perception of risk in a technologically advanced future will be as challenging as it is essential.

There is much the cybersecurity industry can learn from aviation. Managing safety in the face of complex risk has been culturally ingrained into aviation for many years. Achieving this has taken rigorous objectivity and both individual and shared responsibility and accountability. As organizations seek to exploit the opportunities of a connected aviation industry, they must retain the ability to be objective about both the benefits and risks. Innovative connected technologies, if sympathetically and securely integrated, can assist

in efficiency and safety, but this must not be at the cost of unknown or unacceptable risk.

Though the aviation cybersecurity challenge is firmly rooted in connected technologies, the solutions to this challenge may lie elsewhere. A defensive strategy that is rooted in technological solutions is likely to have a limited shelf life. In a rapidly evolving environment, such a strategy will be akin to running while looking at one's feet. To truly get ahead of the problem, the industry must be bold and look to the horizon and its people.

It is often said for both flight safety and cybersecurity; the value is in the journey not the end state. But Brownian motion is not progress and activity is not advancement. It will take leadership and teamwork to truly look to the horizon with clear purpose and stakeholder unity.

The number of aviation cybersecurity initiatives implemented by passionate leaders is growing in parallel with a strong research community committed to understanding and improving the state of aviation cybersecurity. The conditions are ripe to find alignment, direction, and progress under strong international leadership to ensure a safe and thriving aviation industry in the years to come.

Perspectives

An Aerospace Manufacturing Perspective

The global aviation system is the safest it has ever been. Advances in aircraft design, maintenance procedures, and air traffic control all contribute to strong growth while enabling safe delivery of cargo and passengers across the world. That record of success is generated through consistent effort, cooperation, and collaboration among all stakeholders across government, industry, and the flying public. However, as new technologies emerge, new threats also emerge, threats that require constant vigilance, adapted awareness, and new approaches to ensure continued growth and safety in aviation.

The newest concern for the global aviation system is the potential occurrence of a large-scale cyberattack. While the existing safety standards for transport aircraft provide a robust security posture, the wider ecosystem may be more exposed. Maintaining today's unprecedented level of aviation safety and protecting the reputation of the aviation industry are shared responsibilities of the global aviation stakeholder community. It is critical that we identify and understand the threats to aviation systems and adopt common vision, strategies, goals, standards, implementation models, and international policies to protect against cyberattacks.

This report does an excellent job of identifying issues and calling for a unified, industry-wide approach to the emerging cybersecurity threat. To assure security and prevent potential disruption to the aviation system—while at the same time ensuring that the full potential of connectivity is achieved—requires a concerted effort from manufacturers, service providers, and regulators. Publishing this report is an important first step; now we need to move into action.

To support this objective, the Aerospace Industries Association is currently working on an advocacy effort bringing government and industry stakeholders together to address the evolving threats and establish a cybersecurity framework for aviation, first at the national level, and then worldwide.

AIA has assembled a working group to develop recommendations to address evolving threats to the commercial aviation system, which includes both aircraft and the ground and space-based infrastructure on which they rely. They are reviewing the current cybersecurity environment, including already developed standards, regulatory design requirements, and FAA requirements for national airspace systems. The recommendations will include development of a long-term aviation vision, development of a data-driven risk management approach for the aviation system, and defining the measures of success.

Maintaining the safety and security of the global aviation system is a top priority for AIA and its member companies. Sustained growth in aviation is key to unlocking our industry's great potential to create high-skill, high-wage jobs. We look forward to working with government and across industries to address the threat of a large-scale cyberattack against aviation targets and both sustain and enhance confidence in the safety of the global aviation system.

Lieutenant General (Ret.) David F. Melcher is president and chief executive officer of the Aerospace Industries Association (AIA), the premier education and advocacy organization representing the aerospace and defense industry. As AIA President and CEO, Melcher develops the strategy for the association and works with member CEOs to advocate for the industry on behalf of its more than 340 member companies. Melcher joined AIA from Exelis Inc., where he served as CEO and president of a $5+ billion revenue company that was spun off from ITT Corporation in 2011, and ultimately merged with Harris Corporation in 2015. Melcher joined ITT Corporation in August 2008 after a successful thirty-two-year career in the United States Army. He is a recipient of the Army's Distinguished Service Medal, and in October 2014, he received the Association of the US Army John W. Dixon award for contributions to the defense industry.

A Cybersecurity Researcher Perspective

How do you envision the future of your segment, and how do connected technologies play a role?

Supply chain management, third-party penetration testing, and aircraft domain (enclave) management must evolve, and are paramount to the future safety of "e-Enabled" aircraft against cyberthreats. Managing the entire supply chain of components and systems that are integrated into an aircraft is critical. A vulnerable or compromised system from a supplier that makes its way onto an aircraft can be used to attack other connected systems on the aircraft. A risk management framework should be established, followed, and managed for all aircraft suppliers.

Third-party penetration testing should be performed against supplier components and systems, as well as the integrated systems on the aircraft. A third-party is necessary to provide impartial testing. Penetration testing reduces risk and uncovers flaws and vulnerabilities often missed by automated vulnerability scanning tools. Thorough third-party penetration testing should be mandatory for all suppliers for aircraft manufacturers.

Aircraft systems are placed in domains. Systems in each domain have specific Design Assurance Level (DAL) requirements based on system criticality pertaining to hazard analysis or effect on safety of flight. Cybersecurity risk is introduced by the interconnections of these domains, such as data flows between systems at a lower DAL to systems on a domain with a higher DAL. These data flows and rationale for their existence need to be assessed thoroughly.

A risk management framework should be established, followed, and managed for all aircraft suppliers.

What are the major concerns your sector has from a cyber safety, policy, or security standpoint?

The major concerns are cybersecurity awareness, skills shortage, and policy. With cybersecurity awareness, many stakeholders do not understand the true risk connected systems pose to aircraft safety. Risk is often viewed in terms of the current state of affairs, but aircraft systems are complex and are not easily "patched." As an example, everyone thought WPA2 was secure, until KRACK, and that Bash was secure until Shellshock. If a threat tree used to assess risk determined a "low" risk rating for a system using Bash, for instance, how does a major Bash exploit like Shellshock alter this risk rating and what other systems are now exposed in that same threat tree?

Skills shortage is another concern in the aircraft manufacturing industry. The EASA and FAA certify aircraft via type certifications to determine airworthiness of an aircraft "design." The FAA and EASA have done a great job with this in the past, but do they have the cybersecurity expertise to determine if the cybersecurity aspect of the aircraft is properly designed? Aircraft are complex systems with thousands of components from hundreds of suppliers. Adequate cybersecurity skills, training, and experience are required to properly assess aircraft cybersecurity and focus on what has been proven to reduce cybersecurity risk, especially from a fundamental secure design aspect.

Policy is another concern with aircraft manufacturing. Once a type certificate is issued for an aircraft, according to policy, the design cannot typically change. How does this policy address cybersecurity issues in a timely manner, such as applying patches to aircraft systems to mitigate cybersecurity risk? And, what effect does a "patch" to a component on an aircraft have against the entire system? Aircraft are very similar to SCADA systems; both used to be treated as standalone, air gapped systems, but they have both evolved to be connected to the Internet, which introduces a myriad of threats via new entry points into the system. Attacks on the once thought secure SCADA environments are now commonplace—Stuxnet, the Ukrainian Power Outage, etc. Efforts need to be made to ensure attacks such as these do not become commonplace on aircraft.

As technology evolves, how is your sector anticipating and avoiding future threats over the lifetime of those technologies?

Proper risk assessment is critical for aircraft safety. The challenge is when the likelihood of attack against a system that may cause catastrophic impact deemed "rare" or "out-of-scope" later becomes "trivial" due to a new exploit discovery. This evolving risk and how to address it creates opportunities with a certification process that is based on a point-in-time design. To overcome some of these challenges, some aircraft

manufacturers perform risk analysis with the assumption that a system with an external entry point will be fully compromised by an attacker. This helps ensure any system with a connection, or path, from the component considered fully compromised is properly assessed for risk and thoroughly tested.

Software on aircraft is typically treated as a "part." This facilitates configuration control because existing parts management infrastructure and procedures are utilized. A known configuration that is tightly controlled is much easier to assess from a risk perspective, than a system lacking configuration control.

Christian Espinosa is the CEO and founder of Alpine Security. He has worked as a network and systems engineer, a white hat hacker, a trainer, a consultant, and an entrepreneur in the cybersecurity industry since 1993. He has held over twenty industry certifications, including the CISSP, CISA, CEH, CSSA, ECSA, PMP, CCSP, MCSE, etc. He is a veteran of the United States Air Force and holds a BS in engineering from the US Air Force Academy (USAFA) and an MBA in computer and information management from Webster University. He also holds multiple patents on cybersecurity attack and defense simulation. Some of the major recent projects Christian has worked on include penetration testing and security assessments of commercial aircraft, medical device penetration testing, and numerous incident response projects. When Christian isn't protecting us from cyber criminals, he climbs mountains, travels the world, teaches outdoor wilderness survival, and races Ironman triathlons.

An Airport Perspective

The aviation industry is an information ecosystem in which a wide range of stakeholders regularly interact and depend on each other in a "just-in-time" manner, sometimes with little spare capacity to absorb disruptions. The system is highly dependent on and driven by computer systems owned by airports, airlines, tenants, and our federal partners such as FAA, TSA, and CBP. We also need to be conscious of smaller vendors whose systems could be used as an attack vector or could themselves be taken offline, possibly disrupting systems and operations more broadly across the industry.

But aviation is unique in that the industry depends on consumer confidence, particularly in the safety of air travel. Moreover, no other mode has the global reach that aviation does. An attack on airport or airline systems can cause a loss of confidence from the public on a global scale.

Cyber threats are just one of many safety and security issues that are a top priority for airport operators. These include perimeter security systems; public area security; passenger, employee, and checked baggage screening; employee and tenant background checks; and development of airport emergency plans that ensure we are prepared to respond and recover from events when they occur.

In the context of cybersecurity we often think of complex and sophisticated hackers and hacking techniques. But the human element in cybersecurity in our own companies cannot be overlooked. In an airport, employees have legitimate access to large amounts of sensitive data that is attractive to cyber criminals, fraudsters, and terrorists. Staff at all levels, both customer facing and "behind the scenes," are vulnerable to an attack. Our members take these threats very seriously and many have been incorporating cybersecurity awareness into their overall security training programs.

But cybersecurity is not only the protection of personal or sensitive information or any form of digital asset stored in a computer or in any digital memory device. It is also the protection of physical IT assets from attacks targeted to destroy or disable computing power or systems. Think about the exposure at the airport—the airport's own IT network, baggage systems (especially with the increased use of hand-held devices), access control systems, parking management systems, CCTV, perimeter intrusion systems, eEnabled aircraft systems, document management systems (such as electronic Airport Layout Plans), and radar systems, just to name a few vulnerabilities.

Managing these complex cyber risks requires effective sharing of information on vulnerabilities, threat intelligence, mitigation measures, and incident reporting.

ACI-NA routinely provides its members information from DHS and the FBI about the latest cyber threats and mitigation measures. In partnership with the Department of Homeland Security, ACI-NA encouraged airports to take advantage of the Department's Aviation Cyber Initiative, which involved an assessment of potential wireless cyber vulnerabilities. A compilation of the results of the assessments is posted to a secure TSA website for airports to review.

However, the industry still needs its own robust policies and procedures to share cybersecurity information. ACI-NA is working to facilitate the exchange of this information through our Business Information Technology Committee. Our member airports also participate in a worldwide alliance to harden the system through Airports Council International - World, based in Montreal. ACI - World has an active Information Technology Committee addressing these issues.

Additionally, the Airport Cooperative Research Program that is part of the Transportation Research Board and funded by the Airport Improvement Program developed an "Airport Cyber Security Best Practices Guidebook." The results of this research are available online in a guidebook and multi-media material on the TRB website. The goal is to help airports of all sizes establish and maintain an effective cybersecurity program.

There is always work to be done for more effective communications and information sharing to keep up with the bad actors. First and foremost, sustained, sufficient, and secure funding is essential for ensuring that airports can address cyber threats.

We also need to collectively improve how we share information regarding rapidly evolving cyber threats both in the United States and globally. And we need to work not only on preventing cyberattacks, but also on minimizing their impacts on critical infrastructure and making sure we have effective mechanisms in place for containing, responding, and recovering from attacks.

Christopher R. Bidwell is the Vice President of Security at Airports Council International - North America (ACI-NA). He is responsible for leading the association's efforts on airport security, facilitation and oversight of ACI-NA's regulatory activities. He monitors domestic and international aviation security developments, as well as regulatory actions and programs affecting security and facilitation at North American airports. He also serves as committee secretary to ACI-NA's Public Safety and Security Committee.

Air Traffic Control Perspective

How do you envision the future of your segment, and how do connected technologies play a role?

New technologies bring new challenges—this truth is no different for cybersecurity. As aircraft of all types become 'nodes' in the sky, aviation entities around the world will have to work together to mitigate cybersecurity risks. The threat from cyber wrongdoers on one side of the world has the potential to affect aircraft on the other side. No longer will air navigation service providers (ANSPs), airlines, airport authorities, and private aviation be able to stand alone in their approach to the cybersecurity risk. From choosing the most effective remediation to operational response, all aviation must act together. Operation centers must be in constant communication with each other as well as pilots encountering unusual operations. Unmanned aerial vehicles and spacecraft must be part of the community protecting airspace safety.

What are the major concerns your sector has from a cyber safety, policy, or security perspective?

Policies are usually generic and provide a variance of requirements for security, whereas aviation systems are very specific in their operational aspects. For all sectors, cybersecurity investments compete with other technology needs from basic refresh to technical redesign. The challenge of finding a cybersecurity solution that is both affordable and reduces the risk of major cyber threats is compounded by the ever-changing threat and advancements of cyber risks as well as cyber criminals. We are realizing our best deterrents are detecting cyber anomalies and rapidly responding and removing them.

As technology evolves, how is your sector anticipating and avoiding future threats over the lifetime of those technologies?

Future technology must be designed to allow updates in real time. This capability will allow security vulnerabilities to be mitigated as soon as the manufacture provides a remediation. Some of the technology will contain self-healing capabilities. These new functions allow for continuous monitoring and mitigation

throughout the system lifecycle. To cover zero-day attacks, operations will recognize slight changes in aviation tracking as self-healing software keeps the vulnerability to a working minimum. This demands a robust training initiative at operations, supervisory, and management levels to ensure we can quickly recognize an abnormality and act effectively in a timely manner.

Peter F. Dumont is president and CEO of the Air Traffic Control Association. Mr. Dumont has had a career of more than 30 years in aviation ranging from his beginnings as a U.S. Navy air traffic controller to Chief Operating Officer (COO) of the North American sector of a $3 billion defense contracting services company. After retiring from the Navy, Mr. Dumont began his private sector career with Serco, Inc., where he served as Vice President of Aviation and later COO. During his tenure, he oversaw airport management contracts, air traffic control (ATC), ATC equipment installation, meteorology, weather observation, ATC engineering, control tower fabrication and installation, air traffic management (ATM), and business development. Mr. Dumont has been published in a number of ATM-related articles and has provided numerous interviews. Mr. Dumont holds a Bachelor of Science in Professional Aeronautics and Master of Science in Aviation/Aerospace Management, both from Embry-Riddle Aeronautical University.

A Military Perspective

I spent a majority of my Air Force career flying fighters and rarely was I ever concerned for the security of the aircraft systems and associated equipment. My lack of concern likely stemmed from the lack of even knowing I should be concerned. Since then, I have learned the importance of securing these systems, as have others in the military and civilian sector. I now appreciate the risk vulnerabilities these systems pose to successful military operations, particularly when connecting these systems to one another.

Similarities between the military and commercial aviation industry exist and provide synergistic benefits when addressing the vulnerabilities inherent in connected systems. Each has the ability to learn from the other's differences.

My appreciation developed as my experience with and understanding of military planning increased and I learned the value of looking at all aspects of how any threat could affect operations. The primary mission of any military is to defend the nation it serves, and failure to do so results in dire consequences. Extensive and detailed planning occurs to ensure the military is able to respond to and prevail over all possible threats to national security interests. Realistic modeling and war-gaming enables military commanders to examine the various methods an adversary could use to gain an advantage during the lead up to a crisis or during open conflict. These examinations occur across a variety of adversaries to develop an understanding for where vulnerabilities are common no matter who is trying to exploit them or what their motivation or intent may be. As a result, commanders are able to determine their own most critical assets and networks, then prioritize resources to mitigate vulnerabilities in those areas to provide the best returns on their investments. While laborious and seemingly pedantic, military planning greatly assists the system of systems approach to understanding and mitigating vulnerabilities in connected systems.

However, this same level of detailed military planning is not necessarily required of the commercial aviation industry, nor is it likely to be financially feasible. What is likely to be most valuable, and certainly within the realm of feasibility, is a similarly comprehensive approach to securing connected systems that goes well beyond simply ensuring the security of individual pieces of equipment. Industry assesses risk just as the military does by determining the severity of a possible loss and the probability of that loss occurring. Risk assessments against specific actors typically occur for nation-states, transnational organized criminals, and terrorist groups. Nation-states have shown a high probability to exploit vulnerabilities to gain intellectual property, but without lives being put into danger, the severity of those activities is typically thought of as being fairly low. Transnational organized criminal groups have demonstrated their willingness to hold systems for ransom, but, again, the severity of these activities to date has been relatively low. On the other hand, terrorist groups have demonstrated a willingness and capability to gain physical control of an aircraft, with

severe consequences. In today's highly-connected aviation ecosystem, these threat actors can use the same technique to exploit the same vulnerability for their particular purposes. There is now much less distinction between threat actors and the type of tool they may use. Defending against only one "type" of threat is no longer viable, hence the need for taking a more comprehensive, networked approach to risk assessments.

Even if this more comprehensive, actor-agnostic approach to risk assessments becomes the norm, cooperation remains the key to its success. While the military usually brings niche capabilities to bear on a large scale, diplomatic, economic, and information elements of national power are certainly preferred. We are accustomed to providing our capabilities in a supporting role, while also remaining ready to take the lead when called to do so. This same level of cooperation is needed across the commercial aviation industry. No one company, or even government for that matter, can solve this problem on its own, as each is an integrally linked part of the greater aviation ecosystem. Industry should not wait for government-issued regulatory minimums to drive their actions when those will only arrive too late to prevent a catastrophic incident. Industry needs leadership to develop the relationships and, more importantly, the trust that will enable the critical thinking and willingness needed to act effectively.

Similarities between the military and commercial aviation industry exist and provide synergistic benefits when addressing the vulnerabilities inherent in connected systems. Each has the ability to learn from the other's differences. Adopting wide-ranging, more inclusive approaches to securing systems and assessing risk across networks, along with greater trust and cooperation, serve as useful approaches in addressing the information security concerns the commercial sector faces.

Steve Luczynski recently retired from the US Air Force. After a career flying F-15 and F-22 fighters, he transitioned to cyber policy where he was the deputy director for cyber plans and operations in the Office of the Secretary of Defense at the Pentagon. In that role, Steve oversaw the integration of the Department's cyber capabilities and forces into operational plans to defend against and prevail over foreign adversaries. Working closely with National Security Council staff and interagency partners, he contributed to the development of national-level policies to counter foreign cyber threats and protect US interests. He created and led Department-wide initiatives to ensure compliance with presidential directives and enable military cyberspace operations. Steve played a key leadership role in the Department's increasing support to the US government's work to address aviation cybersecurity.

About the Author

Pete Cooper (MSc, CISSP) is an independent cyber security adviser based in London, UK, and a nonresident senior fellow at the Atlantic Council's Cyber Statecraft Initiative.

The first part of his twenty-four-year career in the UK Royal Air Force (RAF), was as a fast jet pilot and instructor on the Tornado GR4. He then became an early member of the UK Ministry of Defense (MoD) Joint Cyber Unit, developing and integrating cyber operations into UK and MoD processes. His final position was in MoD Joint Forces Cyber Group where he was the Strategic Cyber Operations advisor, playing a key role in developing policies, concepts, and doctrine both nationally and internationally.

He has an MSc in cyberspace operations from Cranfield University. His dissertation on adding a cognitive dimension to Active Cyber Defence was published by the Journal of Law and Cyber Warfare and explored how a better understanding of attacker psychology could be used to augment legal Active Cyber Defence methodologies.

Since leaving the RAF in 2016 he has been advising nationally and internationally on cyber security challenges and opportunities, supporting various organizations in developing their strategies. He is also a passionate supporter for the Cyber 9/12 policy and strategy competition, which has seen him present and judge at competitions in both the US and Europe. As director of Cyber 9/12 UK, he is also leading the rollout of the competition in the UK.

Atlantic Council Board of Directors

Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org