AACO/IATA Technical Forum

2019 - Kuwait

Cyber Security and AVSEC:

An International Perspective

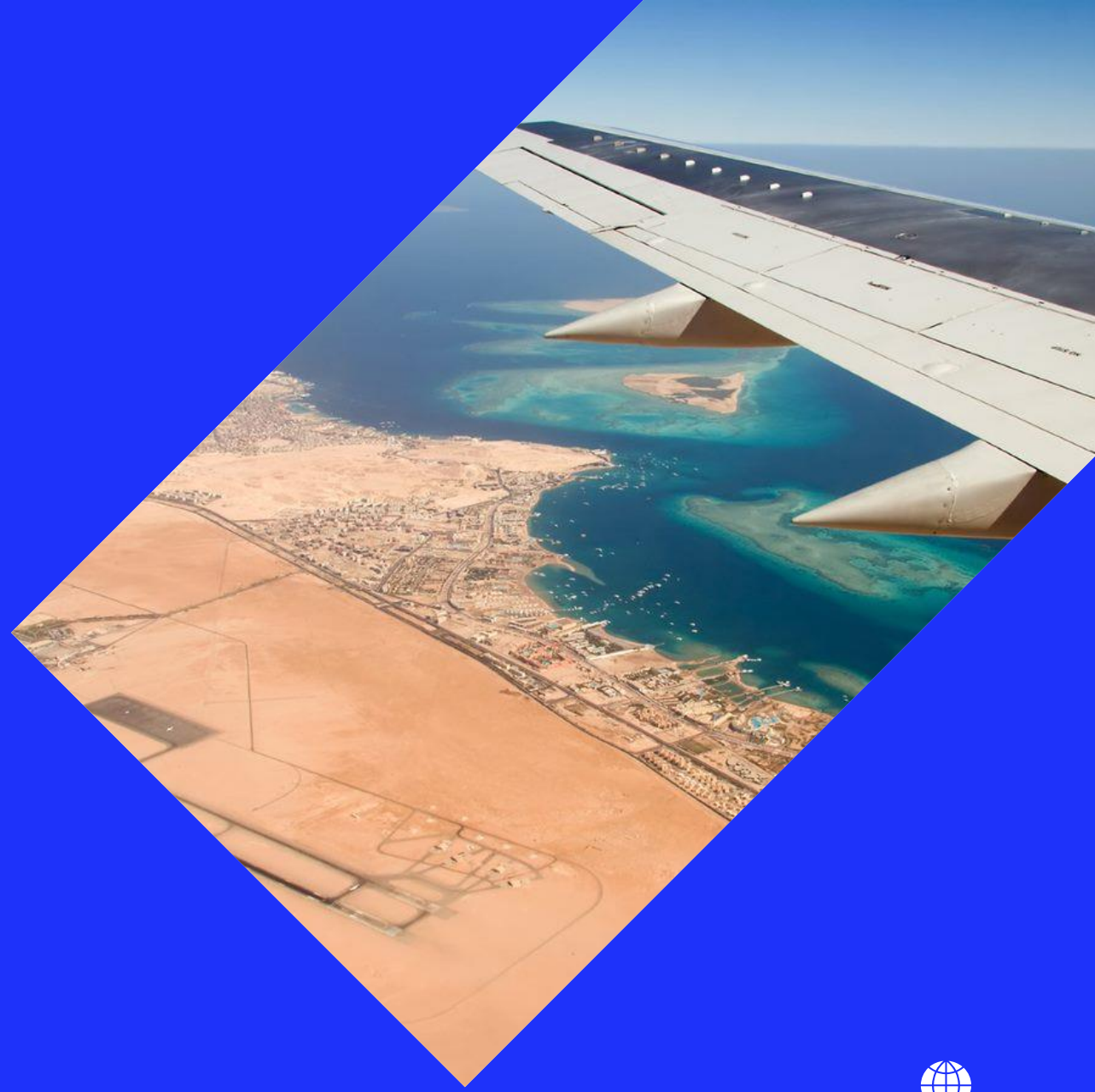
Shawn Goudge

Regional Manager AVSEC - AME, IATA

October 1 – 2, 2019

Contents

- Cyber Security and AVSEC
- Global Initiatives for Cyber Security and AVSEC
  - ICAO Global Aviation Security Plan (GASeP) and ICAO Aviation Cybersecurity Strategy
  - Airports Council International (ACI) initiatives on Cyber Security
  - IATA Initiatives on Cyber Security
    - Working Paper on Cyber Security
    - IATA Cyber Security Position
    - IATA Aviation Cyber Security Roundtable
- Cyber Security – Complexity & Connectivity



Cyber Security and AVSEC

- Aviation cyber security (cyber security that pertains to maintaining safe, secure and resilient flight operations), remains a key priority for the sector.
- The interconnectivity between information technology and other processes show that aviation security and cyber security should not be in individual silos and need to be integrated and cyber security vulnerabilities need to be considered in the AVSEC risk assessment process.
- “Aviation Cyber Security” may be defined as cyber security pertaining to aircraft and airport operations.
- Aviation Cyber Security may be considered as the convergence of people, processes and technology that come together to protect civil aviation organizations, operations and individuals from digital attacks.
- Understanding that not all risks can be known or fully mitigated, adequate resilience to digital attacks and ensuring the continuance of safe aviation operations is a key element of cyber security.

ICAO Global Aviation Security Plan (GASeP)

In September 2016, delegates at the 39th Session of the International Civil Aviation Organization (ICAO) Assembly agreed that there was a need for the accelerated development of a Global Aviation Security Plan (GASeP) as a future aviation security policy and programming framework.

The GASeP, which replaces the ICAO Comprehensive Aviation Security Strategy (ICASS), addresses the needs of States and industry in guiding all aviation security enhancement efforts through a set of internationally agreed priority actions, tasks and targets.

The GASeP provides the foundation for States, industry, stakeholders and ICAO to work together with the shared and common goal of enhancing aviation security worldwide and achieving five key priority outcomes, namely:

a) enhance risk awareness and response;
b) develop security culture and human capability;
c) improve technological resources and innovation;
d) improve oversight and quality assurance; and
e) increase cooperation and support.

GASeP Specific Measures / Tasks Related to Cyber Security

Identify and address cybersecurity threats to civil aviation's critical infrastructure, data and information and communication technology systems through collaboration using horizontal, cross-cutting and functional approaches to achieve an acceptable and commensurate cyber resilience capability on a global level.

It should involve air navigation, communication, surveillance, aircraft operations and airworthiness and other relevant disciplines to ensure the safety and security of civil aviation operations in full alignment with ICAO's Global Air Navigation Plan (GANP) and Global Aviation Safety Plan (GASP).

When considering aviation security risks and measures, ensure appropriate holistic consideration of the aviation sector. Where relevant, early and appropriate coordination with aviation safety, air navigation and facilitation experts to take place at global and national levels.

ICAO Cybersecurity Strategy

- The Strategy is built on ICAO's vision for global cybersecurity – that the aviation sector should be resilient to cyber-attacks and remain safe and trusted globally, whilst continuing to innovate and grow. It will need to be supported by an action plan to be developed through appropriate mechanisms.
- The Strategy is the outcome of deliberations in the Secretariat Study Group on Cybersecurity
- The Aviation Cybersecurity Strategy considers and complements other cybersecurity-related ICAO initiatives. It aligns with existing safety and security Standards and Recommended Practices (SARPs) related to cybersecurity and the protection of aviation critical information, in particular related to Annex 17 — Security

ICAO Cybersecurity Strategy

The Strategy aims for:

a) the protection of civil aviation and the travelling public from cybersecurity threats that might affect the safety, security and trust of the air transport system;

b) maintaining or improving the safety and security of the aviation system in preserving the continuity of air transport services;

c) States to recognize their obligations under the Convention on International Civil Aviation (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity threats; and

d) coordination of cybersecurity measures among State authorities to ensure effective and efficient management of cybersecurity risks.

ICAO Cybersecurity Strategy

- The Cybersecurity Strategy will need to be supported by an action plan, including tangible steps to achieve a mature cybersecurity framework.
- The action plan will draw from guidance on how to implement existing cybersecurity-related SARPS, but will expand on and synthesize these to provide comprehensive guidance on how to achieve the highest degree of cybersecurity.
- The Strategy takes account of existing global plans and further recognizes the need for trained and competent personnel with experience in both aviation and cybersecurity.

ICAO Secretariat Study Group on Cybersecurity (SSGC)

ICAO established the Secretariat Study Group on Cybersecurity (SSGC) and several related Working Groups, composed of subject matter experts from Member States and industry. The SSGC:

- Serves as the focal point for all ICAO cybersecurity work;
- Defines relevant areas to be considered by the Working Groups of the SSGC and validates their respective terms of reference to ensure that no overlapping of duties and responsibilities occur;
- Is conducting a review of ICAO Annexes to consolidate existing Standards and Recommended Practices (SARPs) related to cybersecurity;
- Reviews the proposals for amendments to ICAO provisions or new provisions to be developed related to cybersecurity proposed by the Working Groups;
- Encourages the development of, and participation in, government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts; and
- Promotes cybersecurity awareness throughout the aviation community.

Airports Council International (ACI) – Submission to ICAO

ACI has presented a Cybersecurity working paper to ask that the ICAO 40th Assembly to:

- support the ICAO Aviation Cybersecurity Strategy which has been drafted by the Secretariat Study Group on Cybersecurity (and presented to the Assembly)
- require that ICAO work with States and industry to develop an action plan in support of the strategy
- recognize the immediate need for a multi-disciplinary approach to cybersecurity
- request ICAO to rapidly complete an assessment of the current governance structure for cybersecurity, with serious consideration for a Panel responsible for cybersecurity that considers security, safety, resilience and operational continuity issues together, and
- request that Council involve the industry as well as States when defining policy, a strategy, plans and standards for aviation cybersecurity.

IATA Aviation Security Strategy and Objectives for implementation of the GASeP

IATA has identified 5 Aviation Security Strategy and Objectives for implementation of the GASeP, with the fifth priority related to cyber security:

•Strategic P5 - Develop an industry-led Cyber/digital security strategy with the core focus on preventing and defending against intentional acts of electronic interference and/or acts of unlawful interference.

IATA Submission to ICAO on Cyber Security

IATA has presented a Cybersecurity working paper to ask that the ICAO 40th Assembly:

- IATA strongly supports the position of ICAO as the most appropriate organization to drive coherent global dialogue and action on aviation cyber security.
- Without clear international leadership on aviation cyber security, we risk fragmentation of global standards, a complex regulatory regime that stifles growth and innovation as well as restricting the ability to assess and manage aviation cyber security risk within and across borders.
- This working paper encourages ICAO to*, inter alia*:
  - Recognize the findings from the IATA Aviation Cyber Security Roundtable.
  - Promote the generation of a cyber security culture across the aviation sector following the same model as safety and security culture.
  - Build dialogue, consensus and consistency on both the risks and solutions to aviation cyber security across all international stakeholders, including senior decision makers and risk owners.

IATA Cyber Security Position

IATA Internal Governance and Structures

- As part of the formal IATA governance the newly formed IATA Security Advisory Council (SAC) will advise and guide IATA towards answering the cyber security challenges and opportunities faced by IATA and its airline members.
- The SAC will identify pain points, endorse the development of SARPs as well as speak with one voice to improve cyber security posture and reduce complexity.

IATA Aviation Cyber Security Strategy and Vision

- In consultation with IATA leadership, members and industry partners, an IATA Aviation Cyber Strategy and Vision is to be developed.
- Alongside the IATA Aviation Cyber Security Strategy and Vision, a delivery roadmap will lay out how the strategy is delivered.

https://www.iata.org/policy/Documents/aviation-cyber-security-position.pdf

IATA Cyber Security Position

Stakeholder Engagement

- IATA will engage with its members, industry leaders and stakeholders to develop and subsequently communicate the IATA role and vision in global aviation cyber security.
- IATA will ensure that appropriate partnerships are established that will enable the IATA Aviation Cyber Security Strategy and Vision to be delivered.

Aviation Cyber Security Action

- Taking industry insight, gained during the successful IATA Aviation Cyber Security Roundtable, held in April 2019 in Singapore, some actionable short-term cyber security steps and actions should be identified and conducted by IATA.
- This will not only assist in reducing of cyber security risks but also ensuring that levels of safety and security remain high during the digital transformation of our industry

https://www.iata.org/policy/Documents/aviation-cyber-security-position.pdf

IATA Aviation Cyber Security Roundtable

During the IATA Aviation Cyber Security Roundtable held in Singapore in April 2019, international attendees from across the sector highlighted both where progress is being made as well as where more effort was required. The salient points are laid out below.

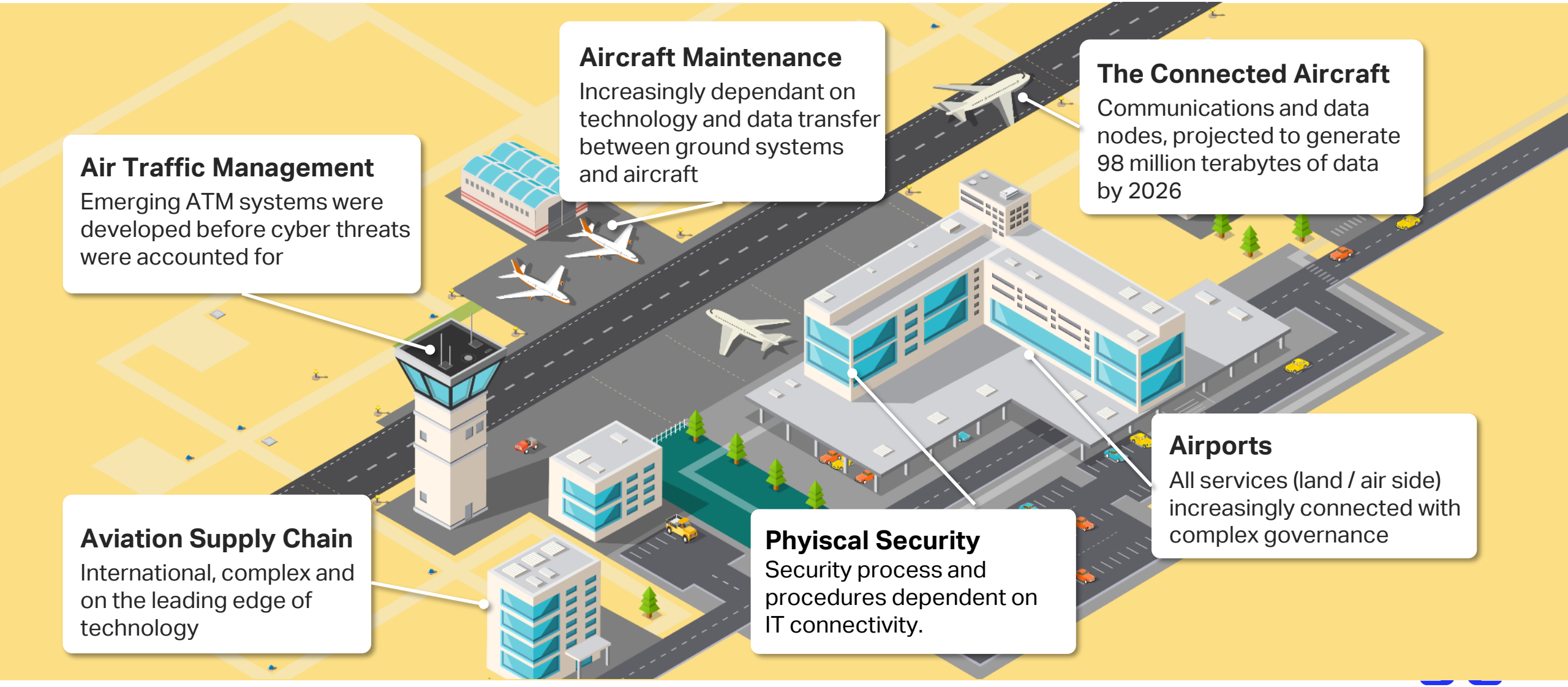
Offered perspectives on the current state of aviation cyber security were;

a) The scale and complexity of aviation cyber security risk is proving challenging for some organizations to understand, prioritize and action.

b) Due to the interdependent and global nature of the aviation sector, it is assessed that cyber security incidents could likely scale rapidly and cause impacts internationally.

c) There remain inconsistencies and insufficiencies across the aviation sector in finding, managing and communicating about cyber security vulnerabilities, leading to poor visibility of actual cyber security risk.

Cyber Security – Complexity & Connectivity - Threat Surface in the aviation ecosystem



Air Traffic Management
Emerging ATM systems were developed before cyber threats were accounted for

Aircraft Maintenance
Increasingly dependant on technology and data transfer between ground systems and aircraft

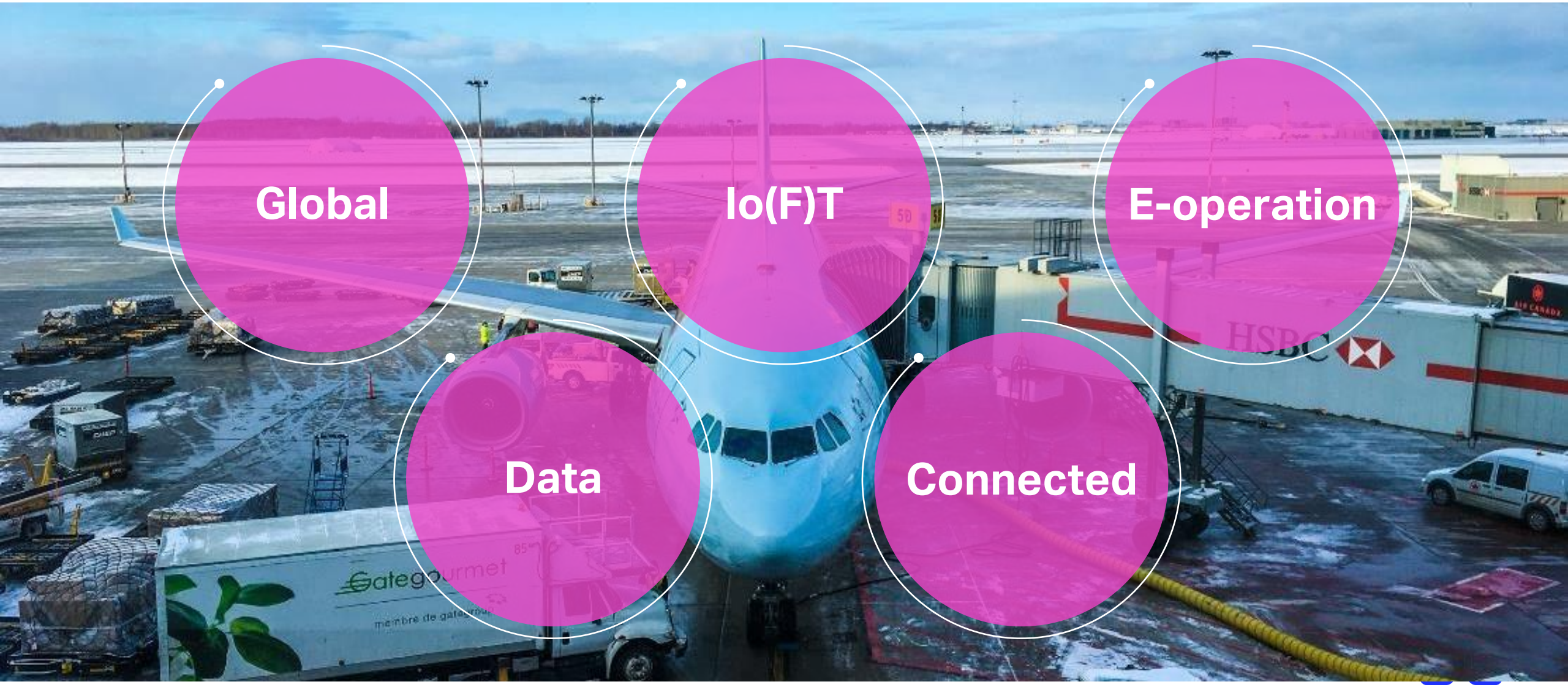
The Connected Aircraft
Communications and data nodes, projected to generate 98 million terabytes of data by 2026

Airports
All services (land / air side) increasingly connected with complex governance

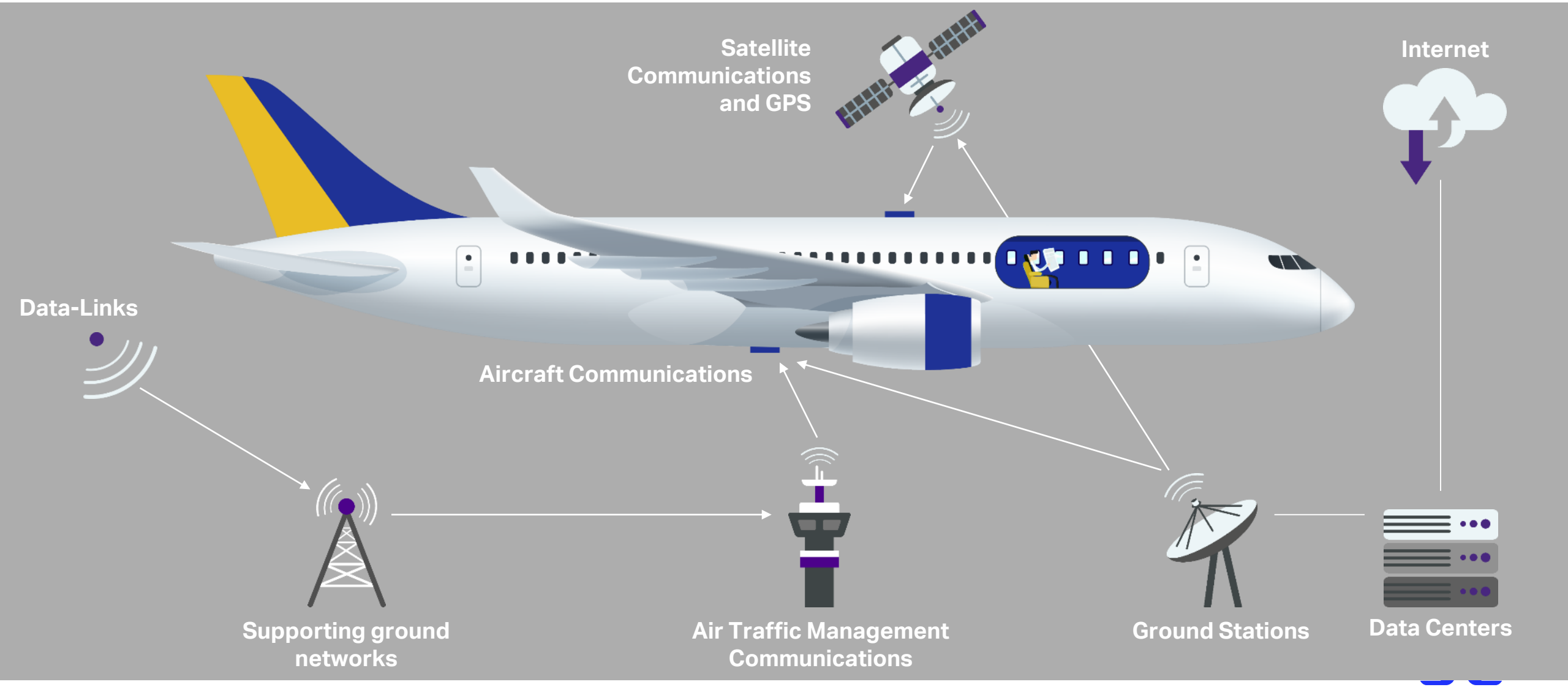
Aviation Supply Chain
International, complex and on the leading edge of technology

Phyiscal Security
Security process and procedures dependent on IT connectivity.

Aviation now and future ...with digitisation



Cyber Security – Aircraft Connectivity



Future Vision for Aviation Cyber Security in 2030

a) Cyber Security Culture. Much like a safety culture and a physical security culture, the whole aviation sector needs a cyber security culture.

b) Transparency and Trust. Between all aviation sector stakeholders, there needs to be increased transparency and therefore trust, on cyber security issues ranging from access to cyber security relevant data to secure development practices and vulnerability management.

c) Building consensus and consistency. Across the global aviation sector we need to further build cyber security consistency, standards and governance.

d) Communications and collaboration. To better manage aviation cyber security risk globally, stronger relationships must be built across the aviation sector as well as with those outside the sector that can assist. This

e) Workforce. Aviation personnel must be taught how to recognize and manage cyber security risks, leading to increased vigilance and resilience.

Relationship Between AVSEC & IT Security

- They key to cyber security from an aviation security (AVSEC) perspective is that cyber and information-technology need to need to be integrated with existing AVSEC processes and procedures.
- This is particularly important where AVSEC functions rely on computers, networks and other information-technology functions.
- All areas outlined in an air operator security program (AOSP) need to be examined from a cyber-security process.

Conclusion

- On aviation cyber security, IATA, along with the airline industry and all other air transport industry stakeholders, faces a complex, critical challenge that is yet to have a clear answer.
- By taking an active leadership role on this challenge, IATA is in a unique position to systemically reduce aviation cyber security risk for its members across the globe, as well as securing the continued growth of air transport by developing a global cyber security framework as well as standards covering the entire supply chain.
- This will fit into an integrated risk management approach combined with threat intelligence and real time information sharing.

https://www.iata.org/whatwedo/security/Pages/cyber-security.aspx

Questions ?

Thank you

Shawn Goudge

Regional Manager Aviation Security – Africa and Middle East (AME)

Office: +962 6 580 4200 ext. 1334

Mobile: +962 (0) 7 97 333 971

Email: goudges@iata.org

www.iata.org