



**Remarks by the  
Secretary General of the  
International Civil Aviation Organization (ICAO)  
Dr. Fang Liu,  
to the Europe, Middle East and Africa (EMEA)  
Cybersecurity in Civil Aviation Summit**

*(Bucharest, Romania, 7 to 9 May 2018)*

*Ladies and Gentlemen,*

1. On behalf of the International Civil Aviation Organization, I would like to express our deepest thanks to the Government of Romania for providing us with such a lovely setting and facilities for this 2018 Cyber Summit here in Bucharest.
2. Many challenges lie ahead of us in the cybersecurity domain, both regionally and globally, and we will need to jointly pursue cross-cutting and multi-functional approaches to address them.
3. One of these challenges is the increasing reliance of the air transport system on rapidly evolving information technologies, and the threats and risks they pose.
4. The insurance sector, for instance, has placed the combined threats from cyber-crime, IT failure, and database breaches as their number-three global business risk for 2017.
5. In an industry as interconnected as air transport, we cannot lose sight of the fact that a single cyber incident will likely impact multiple companies and stakeholders, to varying degrees and costs.
6. Almost daily, new and more sophisticated digital processes are coming online, ones which impact the efficient management of our network, the ability of airline and airport operators to serve their customers, and even the way that air transport professionals like you and I can connect and cooperate together.

7. Virtually no aspect of aviation, or the way which modern business is conducted, is safe today from unwanted cyber intrusion.
8. When we consider cybersecurity, one of the first new realities we must come to terms with is the fact that its threats are digital, anonymous, and respectful of neither political nor geographic boundaries.
9. Localized, physical acts of unlawful interference are no longer the only threats to air transport safety and security.
10. Cybersecurity was highlighted during the last ICAO Assembly, held at the end of 2016, and this week's event reinforces the importance of our continued focus on understanding and addressing the spectrum of potential targets.
11. I would like to take this opportunity to provide an update on some of the progress being made by ICAO in this respect.
12. Following Assembly Resolution 39-19, a Secretariat Study Group was established to work towards an ICAO policy and strategy on *Cybersecurity in Civil Aviation*. This will be proposed during our next Assembly in 2019.
13. This Study Group has already had two meetings and will hold the third one here in Bucharest, just after this Summit.
14. In the meantime, the regulatory framework continues to progress.
15. Last year, Chapter 18 of the *AVSEC Manual on Cybersecurity* was updated. It now provides comprehensive and detailed guidance to States on cybersecurity issues.
16. More recently, meanwhile, the ICAO Council approved Amendment 16 to Annex 17, elevating the former *Recommended Practice 4.9.1 on Cybersecurity* to a new global Standard which becomes applicable this 16 November.

17. I would also invite you to consider the value to these efforts of the new *ICAO Global Aviation Security Plan (GASeP)*, which was endorsed last November by the ICAO Council.
18. The objectives of the GASeP reflect those of UN Security Council resolution 2309 (2016), which empowers air transport and other security stakeholders to work together to protect the aviation network from terrorist threats.
19. Once finalized, the GASeP will be the primary tool by which we fulfil these roles, and you will note in its roadmap that cybersecurity is the very first task area to be addressed.
20. Successfully managing cyber resilience requires a globally harmonized approach amongst all stakeholders.
21. Agreement is needed on how digital information systems should interoperate, in order to provide an information-rich environment for the aviation community.
22. ICAO feels that the secure and resilient exchange of information required to cope with the needs of evolving aviation activities can be enabled through a trust framework.
23. This would consist of coordinated standards, procedures, methods and agreements for the digital exchange of information between ground-ground, air-ground, and air-air systems, as well as to regulate an identity system.
24. These provisions in turn would support the implementation of Performance-based Navigation (PBN), Information Management (AIM), Flow Management (ATFM), or any other current or projected air transport capability requiring the digital exchange of information between systems in a secure environment.
25. Related communications needs for remotely-piloted and unmanned aircraft systems, high-altitude and outer-space operations, and other emerging issues, are also being addressed in this context.
26. The global nature of the aviation cyber threat points to why ICAO is so uniquely positioned to foster the dialogue needed between States, industry and other stakeholders on this issue.

27. It's also why our Organization's events and panels are the natural forums to unite cyber subject-matter experts and develop a harmonized global framework to deal with cybersecurity.
28. The importance of these threats speaks to why they will be a key topic at ICAO's Second High-Level Conference on Aviation Security, which will be taking place at our Headquarters in Montréal this fall.
29. In this regard I would also recall the initial ICAO Cyber Summit, hosted by the UAE in Dubai last April, where the first Declaration on Cybersecurity in Civil Aviation was signed.
30. It underscored, among other points, that States have a key role to play in cyber preparedness and mitigation; the critical value of cyber information sharing and collaboration among all parties; and the need for rapid adoption by States of the Beijing Convention and Beijing Protocol of 2010.
31. It is encouraging for us to see these priorities being supported at this event, as representatives from Europe, the Middle East and Africa, as well as other parts of the world, come together to progress the much-needed harmonization of cybersecurity efforts.
32. Your Summit will open with high-level discussions from policy makers, from the global, State and industry levels, and then evolve toward more technical content focusing on common risk assessment methodologies and the integration of various systems.
33. I would especially like to highlight the table top exercises we have planned for you on aerodrome cybersecurity, jointly organized by Romania, Finland, Airports Council International (ACI) and ICAO.
34. Having multiple stakeholders of this nature involved in these sessions should be of tremendous assistance in helping you to identify the comprehensive solutions now needed.
35. Another important concern which we need to keep in mind is that cybersecurity involves many types of experts from a wide range of technical fields.

36. Aviation used to be one of just a few industries globally which were very technically inclined, but today it competes with a wide range of industry and service sectors which also have urgent needs to attract committed and skilled technical personnel.
37. To put this into perspective, for just the piloting and controller professions in aviation, we need to hire roughly 67 new pilots and 13 new air traffic controllers *each and every day* globally between now and 2036 in order to satisfy forecast demand.
38. ICAO is addressing this rather acute challenge through our Next Generation Aviation Professionals (NGAP) programme, in unison with our Global Aviation Training (GAT) Office.
39. I would highlight for those interested that our second annual NGAP Global Summit will be taking place later this year in Chengdu, China, and that we hope to see some of you there.
40. Aviation, academic and many other experts will be on hand there to discuss how we attract, retain and manage the international allocation of air transport's future skilled professionals.
41. As we consider this aspect of our cyber-related strategies and planning, 'please let me take a moment to thank Romania for inviting the university students who have joined us here today.
42. I hope that the challenging topics before us help inspire each of them to consider careers in our very exciting and evolving sector.
43. In concluding today, ladies and gentlemen, I would like to call upon each of you to keep in mind how catastrophic even a single cyber event could be for multiple stakeholders in the air transport network.
44. Importantly counted among these are the passengers and shippers who must rely upon the safety, security and on-time performance of air transport for their business-critical or personal needs.
45. I also call on you to recognize that a truly effective cyber stance for global aviation will only be achieved through closer partnerships between us – both States and private sector innovators – as well as via the constant re-assessment of related risks and measures.

46. As was stated with great prescience in the Chicago Convention:

*“The future development of international civil aviation can greatly help to create and preserve friendship and understanding among the nations and peoples of the world, yet its abuse could become a threat to the general security.”*

47. Our job together is to prevent abuses of the air transport network through some of most insidious and difficult to prevent threats we have ever encountered.

48. Air transport is being more and more recognized today as a critical pillar supporting the socio-economic prosperity and sustainability of cities, States and Regions all over the world, so the stakes are high where our effectiveness is concerned.

49. With this in mind, may I wish you all a very successful, engaging and results-focused 2018 Cyber Summit here in Bucharest.

Thank you.