国 际 民 用 航 空 组 织

工 作 文 件

A42-WP/369[1]
EX/154
29/7/25

大会 — 第 42 届会议

执行委员会

议程项目 13：航空安保 — 政策

按照协作工作计划制定航空网络安全战略保护民用航空

（由哥伦比亚提交，拉丁美洲民航委员会 16 个成员国[2]支持）

执行摘要

航空业正在经历前所未有的数字化转型。数字通信、智能系统集成、数据分析、先进监控、预测性空中交通管理系统和云计算等技术都在重塑航空业的面貌。然而，这种日益增长的互联互通也扩大了网络攻击范围，增加了航空业面临网络威胁的脆弱性。日益复杂的网络攻击危及安全、数据隐私和对系统的信任。

为应对这一挑战，加强航空网络安全至关重要。成员国应实施国际民航组织的各项建议，例如《航空网络安全战略》和《网络安全行动计划》，并根据本国国情作出调整，加强组织文化、技术基础设施和网络安全法规，以应对民航领域与网络安全具体相关的挑战。

此外，网络空间具有的交易性质要求成员国之间建立对话以及技术和运营合作机制。

行动：请大会：

a) 要求国际民航组织理事会在其 2026-2050 年战略计划中制定一项自我评估工具，供各国衡量其航空网络安全的成熟程度。

战略目标：	本工作文件涉及以下战略目标： - 每次飞行都安全和安保 - 航空实现无缝、无障碍和可靠的全民出行 - 不让任何国家掉队
财务影响：	
参考文件：	- 附件 17 —《航空安保》 - 国际民航组织文件：《航空网络安全战略》 - 国际民航组织文件：《网络安全政策指导》 - A41-19 号决议：解决民用航空网络安全问题 - 国际民航组织文件：《网络安全行动计划

[1] 西班牙文文本由哥伦比亚提供。

[2] 伯利兹、多民族玻利维亚国、哥斯达黎加、古巴、厄瓜多尔、萨尔瓦多、危地马拉、洪都拉斯、牙买加、墨西哥、尼加拉瓜、巴拿马、巴拉圭、秘鲁、乌拉圭、委内瑞拉玻利瓦尔共和国。

1. 引言

1.1. 在先进技术的推动下，全球航空经历了前所未有的数字化转型。然而，数字化也使网络更易遭受攻击，这能危及系统的安全性和可信度。因此，加强网络安全是保护信息和维持空中持续运营的关键。

1.2. 各国已制定全面网络安全战略，包括人才培训、加强安保技术、建立监管框架、公私合作和国际协作。这项战略旨在全面改善国家劳动力的培训、技术基础设施和风险管理。

1.3. 国际合作是加强航空业抵御网络威胁的关键。信息共享、响应协调和协作机制 — 其重要性在2024 年 7 月 19 日影响全球航空公司管理系统的事件中得到了体现 — 有助于降低风险并确保安全。

1.4. 数字化已使民航业更易遭受网络攻击，危及民航业的安全和基础设施。加强网络安全是确保其连续性和韧性的战略重点。

1.5. 国际民航组织的《航空网络安全战略》和《网络安全行动计划》为应对这些挑战提供了坚实的框架。然而，有效实施这些建议需要在地区层面采取协调一致的持续行动，并需要包括成员国、业界和学术界在内的所有利害攸关方作出坚定承诺，推动国际民航组织 2026-2050 年战略目标的实现。

2. 讨论

2.1. 数字化优化了民航业，改进了流程和竞争力。然而，各系统之间的互联互通也增加了网络安全风险，包括未经授权的数据访问和关键系统遭到篡改。因此，各国必须加强自身能力，并开展合作，增强行业的安全性和信心。

2.2. 民航业面临着在确保网络安全的同时需要利用数字化的好处的挑战。这需要采用数字安全技术、开展员工培训、分享经验并为行业内各企业制定信息和数字安全政策及战略。

2.3. 国际民航组织将网络安全视为一项需要国际合作的共同责任。由于网络威胁演变迅速并跨越国界，各国应以灵活和协调的方式来应对，共享信息、最佳做法和技术资源。

2.4. 针对民航的网络攻击并非是假设性的威胁，而是一个切实存在的隐患。恶意行为者能破坏空中交通管制、导航和飞行管理系统等关键设施，危及数百万乘客和机组人员的安全。此外，网络攻击还会严重扰乱航空运营，造成数百万美元的财务损失，并损害行业声誉。

2.5. 民航面临各种网络风险，包括数据盗窃、系统篡改、关键服务中断和公众信心丧失等。加强网络安全是确保安全可靠运营和维护行业稳定的关键。

2.6. 随着网络攻击的威胁日益加剧，必须采取全面和协作的方式，通过建立强有力的框架来指导各国和利害攸关方实施有效的安全措施，以加强民航网络安全。这个框架应依靠高级管理层的承诺、有效的治理以及明确的网络安全政策来保护关键信息和运营系统。

2.7. 应制定一套流程来加强民航网络安全能力。其战略应建立在四大支柱之上：（i）员工培训；（ii）加强内部技术基础设施；（iii）建立监管框架以促进整个民航业的网络安全；（iv）各实体之间的合作。

2.8. 这项战略旨在通过管理关键系统中的信息完整性、可用性和机密性来促进民航安保，从而确保高效提供服务并通过训练有素的人才保护敏感数据。此外，还应实施强有力的监管框架，以加强航空公司、机场、供应商和制造商的网络安全，促进强有力的安保作法和对网络事件的协调响应，从而在日益增长的数字威胁面前提高韧性并保持用户信心。

2.9. 此外，通过持续的网络安全培训，培养专业人才至关重要。培养合格的专业人员是确保安全和降低员工流失的关键。此外，还需要整合专门的民航网络安全事件响应中心，使民航能快速、协调地应对网络事件。这个中心应成为网络安全事件管理、与行业利益攸关方进行协调以及自身团队培训的枢纽。

2.10. 国际合作是信息共享和开展联合模拟演练以有效应对跨境网络威胁的另一个关键要素。单一的技术平台将促进知识和最佳做法的交流。

2.11. 应与主管部门和行业各企业保持持续对话，以协调统一应对网络威胁。然而，网络空间没有国界，因此，这种对话应涵盖各国，而各国应建立高效和强有力的机制，分享经验并就国家网络安全战略交换建议。

2.12. 国家网络安全战略的关键应以各国的法律和法规为基础，同时又应具有互操作性，确保全球运营安全。应促进专家之间的合作和信息共享，以识别和解决漏洞，增强行业抵御网络攻击的能力。此外，还应创建一个持续进行的论坛，让专家们能够就本地战略提供反馈，并共同努力弥补可能被网络犯罪分子或网络恐怖分子利用的漏洞。

2.13. 在这方面，认为国际民航组织有必要推动加强民航网络安全管理的行动。创建一个自我评估工具并将其纳入《2026-2050 年战略计划》是合理的，因为它使各国能及早发现政策、运营和技术方面的差距，促使其主动规划缓解措施并发展国家能力。这有助于确保各国之间保护水平更加均衡，减少目前全球航空网络脆弱性的不对称现象。

2.14. 同样，国际民航组织也必须推广更具体的网络安全技术和政策指导方针，指导各国采用最佳做法和国际标准。这将有助于构建一个共同框架，以便更有效地应对数字威胁，增强航空系统的韧性，并在全球范围维护空中运营的安全和连续性。

3. 结论

3.1. 民航网络安全是一项需要全球协调应对的挑战。国际民航组织应与其成员国合作，带头提高民航业的安全性和抵御网络威胁的能力。数百万乘客的安全和全球航空系统的稳定都依赖于此。

—完—