国 际 民 用 航 空 组 织

工 作 文 件

A41-WP/64[1]
EX/33
22/7/22

大会 — 第 41 届会议

执行委员会

议程项目 14：航空安保 — 政策

国际民航组织网络安保战略和工作计划的整合与协调

（由国际航空运输协会（IATA）提交）

执行摘要

民用航空网络安保仍然是国际民航组织、各国和业界日益关注的领域。重点不仅在于识别和减少意图干扰数字系统的网络威胁和风险，还在于提供一个采用关键原则（如航空航天业的安全源于设计的原则）的安全技术创新的国际框架。

本文件提出了新成立的特设网络安保协调委员会（AHCCC）在提供网络安保方面采取综合、协调办法的必要性。注意到技术专家组和分组提出的可能会影响标准和建议措施（SARPs）的建议以及其他要求，反映了该学科横向贯穿了国际民航组织众多附件、文件和手册。

行动：请大会要求理事会：

a) 请理事会确保国际民航组织的所有工作机构根据安全源于设计原则，共同创建一个跨学科、多步骤的协同方法，以整合网络安保规定和其他要求；和

b) 请理事会认识到采用不受民航条例和 SARP 约束的新一代互联创新技术和相关供应链的潜在影响。

战略目标：	本工作文件涉及战略目标：安全、安保和简化手续及空中航行能力和效率。
财务影响：	开发、协调和处理将由业界提交给国际民航组织的新规定和指导材料的费用。
参考文件：	Doc 10140 号文件：《大会有效决议》（截至 2019 年 10 月 4 日） Doc 10108 号文件：《航空安保全球风险背景综述》； A40-10 号决议 — 解决民用航空网络安保问题； 航空网络安保战略 网络安保行动计划

[1] 中文、阿拉伯文、英文、法文、俄文和西班牙文版本由IATA提交。

1. 引言

1.1 国际民航组织大会第 40 届会议（2019 年）通过了 A40-10 号决议 — 解决民航网络安保问题。实质上，该决议授权国际民航组织秘书长继续确保本着国际民航组织航空网络安保战略（2019 年）的精神，通过适当机制，以贯穿各领域的方式审议和协调网络安保事项。

1.2 国际民航组织航空网络安保战略提出了一系列原则、措施和活动，并通过后续的国际民航组织网络安保行动计划（CyAP）（2019）务实地确定了明确的协调行动，以应对网络威胁和提高国际民航对数字安全、安保和信任的应变能力所需的要素。

1.3 2022 年，国际民航组织理事会通过了成立特设网络安保协调委员会（AHCCC）和在两个不同委员会下设立两个独立小组的决定。这突出强调了国际民航组织和理事会对战略航空网络安保重要性的重视。航空安保委员会在 2022 年 1 月 24 日第 225 次会议上批准建立新的网络安保专家组（CYSECP），该专家组于 2022 年 5 月举行了第一次会议。CYSECP 注意到了 SSGC 之前取得的成就，并提出了一项工作计划，补充了组织内部和国际协调的必要性。此外，空中航行委员会（ANC）设立了可信系统专家组（TSP），以加强国际民航组织各局、委员会和技术专家组之间的交叉协调。

2. 讨论

国际民航组织网络安保协调

2.1 众所周知，航空网络安保本质上是一个横向的综合学科。因此，AHCCC 的未来作用至关重要，以确保协同的战略方向，将国际民航组织相关工作的工作计划和活动结合起来，最终保护航空免受各种形式的数字干扰，同时支持安全的技术创新。

2.2 从本质上来说，SARPs 以及源自文件的指导意见通常与各国履行 19 个附件中规定的国际义务有关。因此，至关重要的是，AHCCC 通过结构化和高效的治理确保协调。

2.3 下文介绍了与 AHCCC 有关的一些工作：

a) 可信系统专家组的活动基于下一代空中交通的基础，并触及此类框架的运行和治理概念的发展；

b) 网络安保专家组制定活动，考虑引入或提议更改/修改网络安保规定中的现有附件、文件和手册；

c) 信息管理专家组在其《空中航行服务—信息管理程序》（PANS-IM）中表达了某些信息安全要求，也开展了其他工作，如目前正在起草的关于在航空电信网络上实施互联网协议服务的 9896 号文件第三修订稿，该文件还在其手册中引入了网络安保要求；

d) 还建议对《安全管理手册》（Doc 9859）进行修改；

e) 注意到国际民航组织理事会提交的A41-WP/22文件中引用的附件17网络安保相关SARPs与全球安全审计计划（USAP）结果之间的协调；和

f) 注意到国际民航组织理事会提交的A41-WP/22文件提及的法律问题研究小组（RSGLA）的工作以及秘书处与法律委员会的协调。

2.4 随着时间的推移，整合不同附件和文件的网络安保要求和规定将变得复杂。因此，可能有必要评估创建新附件的必要性，以降低整合的复杂性，并确保横向制定 SARPs，以解决缓解蓄意和/或非蓄意事件的措施，更重要的是，可能导致二次/累积安全或安保影响的威胁不一定立即被视为一种数字干扰。

数字化转型整合

2.5 数字化转型正在多个领域不断发展，产生了更多互联技术，如预测性飞机维护、人工智能和/或基于机器学习的决策制定、边缘计算、开放式架构，以及关键电信系统的“空中更新”。

2.6 最新的空中交通概念正在催生新的高效技术。然而，航空航天供应链不一定受传统的国家民航法规和标准的监管。新的供应链带来了不透明机会，使潜在漏洞得以存在，这些潜在漏洞被引入已然复杂的运行环境中，网络攻击的范围曾经局限于历史系统，现在已经扩展到未知的互联技术。总的来说，新出现的互联性和日益增长的依赖性要求清晰的航空航天监管结构，以支持持续的适航性和航空器认证。

2.7 安全源于设计原则是国际民航组织航空网络安保战略中提到的网络安保政策方法的一部分。在这方面，旨在以数字技术保护工业并支持下一代技术、创新产品和服务的工作计划必须是适用不同平台的，并能解决整个民航系统的问题。它不仅仅局限于支持一个信任框架概念或提出对附件和文件的修正，而是一个多阶段方法的总体跨学科工作计划。

3. 结论

3.1 国际航空网络安保政策和义务使受监管的运营商及其供应链能够实现有效的投资回报，这对于航空业的可持续性至关重要。此外，国际民航组织和各国需要支持使行业实现创新并提高民用航空对新供应链的适应能力的国际努力。当务之急是推广安全源于设计的方法，即跨学科和多阶段的方法，从而将民航组织各小组、工作组和研究小组的规定和要求纳入 AHCCC 负责的通用工作计划。

3.2 以安全源于设计为主导的工作计划可以建立一个具有网络抵御力、灵活、创新的综合生态系统的基本基线，以减少针对国家和行业的网络攻击的频率和影响，这些攻击可能对安全和更广泛的国际民用航空业产生影响。

— 完 —