国 际 民 用 航 空 组 织

工 作 文 件

A42-WP/12
EX/4
21/7/25

大会 — 第 42 届会议

执行委员会

议程项目 13： 航空安保 — 政策

民用航空的网络安全

（由国际民航组织理事会提交）

执行摘要

民航部门应对网络威胁和风险的意识和行动一直都在稳步增强。在上一个三年期期间，国际民航组织以及各国在国家、地区和全球层面都取得了许多进展。然而，仍有许多工作有待开展，尤其是在国家层面，以确保在整个民航部门对航空网络安全采取整体、协调和一致的办法。

本文件介绍了与航空网络安全相关的活动，包括大会授权的活动，并虑及国际民航组织就此主题开展的工作，建议更新关于解决民用航空网络安全问题的 A41-19 号决议，以强调提高民航部门防止和抵御网络威胁和风险能力的重要性。

行动：请大会：

a) 注意到航空网络安全活动方面的发展；和

b) 通过附录所载的关于解决民用航空网络安全问题的大会决议。

战略目标：	本工作文件涉及战略目标：每次飞行都安全和安保和航空为所有人提供无缝、无障碍和可靠的出行。
财务影响：	本文件提及的国际民航组织活动将在国际民航组织 2026-2028 年业务计划指导下，根据 2026-2028 年经常预算和/或预算外捐助的可用资源情况开展。
参考文件：	Doc 10184 号文件：《大会有效决议》（截至 2022 年 10 月 7 日） 《航空网络安全战略》 《网络安全行动计划》

1. 引言

1.1 民航部门在使用信息和新技术支持其自动化、互联性和互操作性需求方面，以及在地面和空中部署新的运营概念和将新加入者（如无人航空器系统（UAS））纳入航空运输系统方面，经历了快速发展。这些发展的最终目标是支持民航部门的增长，同时确保其安全、安保、效率、能力和可持续性。

1.2 然而，这一趋势导致对运行系统、数据和信息的网络威胁增加。世界各地的地缘政治紧张局势则进一步加剧了这一增长。虽然尚未有网络攻击对航空安全或安保造成重大影响的报告，但该部门正在面临网络事件报告数量上升的趋势，迄今为止，这些事件似乎主要是由经济利益、信息窃取或黑客活动驱动的。[1]

1.3 日益复杂的网络威胁及其对民航的潜在影响突出表明，需要一种全球性的、强有力的和协调一致的做法来加强民用航空防止和抵御网络威胁的能力。在这方面，国际民航组织继续与各成员国、国际组织和业界合作，支持它们减轻民航部门面临的网络风险。

1.4 国际民航组织大会第 41 届会议满意地注意到国际民航组织在过去三年期（2019 - 2022 年）期间在航空网络安全方面取得的进展，并对国际民航组织及其各专家小组的工作表示赞赏。大会尤其欢迎在国际民航组织内通过并实施强化的航空网络安全内部治理架构，以及持续制定航空网络安全政策、规定、指导、能力建设和宣传举措。国际民航组织大会第 41 届会议还通过了关于解决民用航空网络安全问题的大会 A41-19 号决议，该决议取代了大会 A40-10 号决议。

2. 讨论

2.1 航空网络安全标准和建议措施

2.1.1 2022 年，为回应网络安全行动计划（CyAP）行动项目 CyAP3.4，其中要求国际民航组织“审查国际民航组织的现有标准和建议措施（SARP），以确定潜在的网络安全更新需求”，国际民航组织对《国际民用航空公约》（《芝加哥公约》）的 16 个附件进行了深入的单独分析，目的是确定国际民航组织的标准和建议措施中与航空网络安全相关的潜在关注领域，以支持在国际民航组织规定中对航空网络安全采取整体和跨领域的做法。

2.1.2 分析报告已提交网络安全专家组，该专家组设立了网络安全标准和建议措施工作队（TF-CYSARPS），通过对相关附件中跨航空学科的潜在关注领域进行交叉比对，继续开展工作。工作队的工作旨在调查现行标准和建议措施是否充分涵盖航空网络安全（无论明示或暗示），查明国际民航组织的标准和建议措施框架的潜在差距，并与相关各专家组酌情协调解决这些差距。有关这个主题的工作正在进行之中，预计将在接下来的三年期内持续进行。

[1] 有关民用航空领域网络威胁与风险的进一步信息，请参阅国际民航组织《全球网络风险考虑因素》（Doc 10213 号限制发行文件）。

2.2 国际法律文书

2.2.1 提交给法律委员会第 38 届会议的《国际航空法文书对于针对民用航空的网络威胁的适用性研究》得出结论，认为《制止与国际民用航空有关的非法行为的公约》[2]（2010 年，北京 —“2010 年北京公约”）和《制止非法劫持航空器公约的补充议定书》[3]（2010年，北京 —“2010年北京议定书”）对以往的法律文书作出了重要补充，为各国将针对民用航空的网络攻击作为罪行处理提供了充分依据。

2.2.2 截至 2024 年 4 月 1 日，已有 53 个成员国批准了《2010 年北京公约》，54 个成员国批准了《2010 年北京议定书》。鉴于这两份文书载有与解决针对民用航空网络攻击相关的规定，因此强烈建议成员国广泛通过并批准这两份文书，正如大会关于解决民用航空网络安全问题的决议所强调的那样，以支持遏制针对民用航空的网络威胁并起诉针对民用航空部门的网络攻击。

2.3 全球航空安保计划（GASeP）第二版

2.3.1 根据网络安全计划的行动项目 CyAP2.5，其中要求国际民航组织“将网络安全纳入地区和全球计划，以确保航空安全、安保和应变力”，并借助于 2024 年 6 月发布的全球航空安保计划第二版的更新（https://www.icao.int/Security/Pages/Global-Aviation-Security-Plan.aspx），国际民航组织已将航空网络安全纳入该计划的规定中，置于全球优先事项 1、2 和 4 之下。

2.4 指导材料

2.4.1 根据网络安全行动计划，国际民航组织制定了指导材料，[4]以支持各国和利害攸关方应对民用航空的网络安全问题，其中包括国家层面的航空网络安全治理和政策、民用航空的网络安全文化以及网络信息共享规划和实施的指导。国际民航组织还发布了《全球网络风险考虑因素》（Doc 10213 号限制发行文件），这是一份指导文件，其中提供了将网络风险管理纳入航空安全、航空安保以及空中航行效率和能力风险管理流程的方法，并包含了一份高级别的全球网络威胁和风险形势概述。

2.4.2 根据第 14 次空中航行会议关于航空网络安全的第 4.2/1 号建议，正在进行的指导材料编制工作包括制定一套全面的指导文件，以处理航空网络安全的不同方面。此外，还计划将所有指导材料汇编成《航空网络安全手册》，其中将涵盖有关关键航空基础设施和服务防止和抵御网络威胁和风险的所有方面。

2.5 信任框架

2.5.1 空中航行委员会在其 2022 年 6 月举行的第 220 届会议上批准成立信任框架专家组（TFP）。自那时起，信任框架专家组一直致力于制定建立可互操作的信任框架的指导材料：

---

[2] Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation
[3] Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft
[4] https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx

a) 已制定了用于运行环境的可互操作的信任和身份保证技术指南，包括信息安全指南（Doc 10204 号文件 —《航空信息安全手册》）；

b) 航空通用证书政策，以支持民用航空中可互操作的数字身份、信息真实性和保障，包括但不限于支持全球导航卫星系统（GNSS）星基增强系统（SBAS）的认证；

c) 制定并维护了信任框架发挥益处的运行使用案例清单。最近已开始编制指南，以支持航空利害攸关方制定信任框架实例；和

d) 在相关各专家组密切协调下，正在最终确定通过互联网协议套件的航空电信网（ATN/IPS）进行安保的空地通信的指导材料，以直接支持对附件 10 —《航空电信》第 III 卷 —《通信系统》的第 93 次修订。

2.6 国际民航组织航空网络安全工作方案

2.6.1 理事会在查明充分的秘书处资源以支持 AHCCC 运作后，于 2023 年第 228 届会议上批准 AHCCC 的成立、成员组成和职权范围。AHCCC 的成员包括来自航空运输委员会（ATC）、航空安保委员会（ASC）和空中航行委员会（ANC）的各 1 名成员，以及来自在其工作方案中定期处理网络安全问题的各专家组的 11 名成员。

2.6.2 委员会的主要职能是通过制定和维护一份全面的国际民航组织航空网络安全工作方案，协调国际民航组织各部门间的航空网络安全相关工作。它还作为理事会的主要咨询机构，根据工作方案排定各项工作要素的优先次序。

2.6.3 AHCCC 自成立以来已举行三次会议，并随着网络安全工作的演进继续改进国际民航组织的航空网络安全工作方案，充当各专家组的协作平台，以便共享信息和支持在各自工作领域就航空网络安全问题采取协调一致的方法。

2.7 培训和能力建设

2.7.1 目前，国际民航组织的网络安全培训组合包括两门航空网络安全课程：

a) 航空网络安全领导力和技术管理基础：该课程由国际民航组织与 Embry-Riddle 航空大学合作开发，于 2021 年 10 月开始授课。这是一门全面认知课程，涵盖了《航空网络安全战略》涉及的网络安全问题的各个方面。在上一个三年期期间，于 2022 年 9 月至 2025 年 4 月之间向 88 名学员授课；和

b) 民航网络安全监督：该课程由国际民航组织与联合王国民航局合作开发，于 2023 年 3 月开始授课。课程涵盖了支持各国制定和实施航空网络安全监督框架的各个重要方面，并以联合王国的经验为例。在上一个三年期期间，于 2023 年 3 月至 2025 年 4 月之间向 34 名学员授课。

2.8 提高认识和外联活动

2.8.1 按照国际民航组织大会第 41 届会议要求国际民航组织加强宣传和开展航空网络安全模拟演习的呼吁，本组织得到葡萄牙和新加坡对航空网络安全方案的慷慨自愿捐助，这使得在本三年期期间得以开发和举办五次地区航空网络安全研讨会。

2.8.2 这些研讨会聚集了来自所有航空和非航空相关领域的参与者（航空安全、航空安保、空中航行、网络安全、国家计算机应急小组/计算机安全事件响应小组（CERT/CSIRT）、国家网络安全机构、执法部门、军队等）。研讨会共有超过 450 名参与者参加。

2.8.3 除了作为地区航空网络安全研讨会一部分进行的模拟演习（TTX）外，国际民航组织还在 2025 年 6 月 5 日举行的第四次网络安全专家组会议（CYSECP/4）会外和 2023 年安保周期间进行了一次模拟演习以及四次独立的模拟演习，使国际民航组织在三年期期间进行的航空网络安全国际模拟演习总数达到十次。

3. 修订大会 A41-19 号决议

3.1 继《马斯喀特宣言》通过之后，虑及第 14 次空中航行会议的成果，对大会 A41-19 号决议作出了拟议更新，载于本文件所附附录。与国际民航组织网络安全专家组就更新决议进行过协调，使其符合《马斯喀特宣言》的内容和空中航行会议关于航空网络安全的成果，并符合网络安全专家组第三次会议核准的航空网络安全术语定义，以及国际民航组织在这个主题方面的工作进展。

— — — — — — — —

附录

~~A41-19~~A42-XX：解决民用航空网络安全问题

鉴于国际航空系统是高度复杂和~~综合~~互联的系统，由数据、信息和系统组成，它们对民航运行的安全、~~和~~安保、效率和能力都至关重要~~的系统组成~~；

注意到航空领域越来越依赖数据、信息~~、数据~~和系统的可用性和~~、~~完整性~~和保密性~~，以及在特定情况下其保密性；

认识到航空网络安全对于航空运输的可持续和高效发展至关重要，因此应予以优先重视并提供适当的资源；

~~认识到不是所有影响民用航空安全、安保、效率或能力的网络安全事件网络事件都是非法和/或故意针对民航的；~~

考虑到对民航的网络威胁正在~~快速~~持续演变，其规模、复杂程度和频率都在不断增长，~~并且如同~~在网络和现实领域，航空继续成为~~网络领域犯罪份子~~恶意行为者的目标，并且网络威胁可以~~演变，影响到全世界范围的关键~~对民用航空的关键基础设施造成重大风险~~系统~~，可能危害航空安全、安保、效率或能力；

认识到网络安全挑战和解决方案的多面性和多学科特点，并注意到网络风险可同时影响到和扩散到广泛的航空领域~~并迅速扩散~~；

认识到不是所有影响民用航空安全、安保、效率或能力的网络安全事件网络事件都是非法~~和/~~或故意针对民航的；

重申《国际民用航空公约》（芝加哥公约）规定的义务来确保民用航空的安全、安保和持续性；

考虑到《制止与国际民用航空有关的非法行为的公约》（北京公约）和《制止非法劫持航空器公约补充议定书》（北京议定书）将改进全球法律框架，把对国际民航进行网络攻击作为犯罪行为~~应对~~，因此~~各国~~成员国广泛批准和实施这些文书将确保这些攻击无论发生在~~世界~~何处，都会受到震慑和惩罚；

重申~~解决~~加强民航关键~~系统、数据和信息~~数据、信息和系统的保护以~~防止和~~抵御~~网络安全和网络复原力不受~~网络威胁和~~危险~~风险的重要性和紧迫性，包括民用~~和军用~~航空与其他相关部门之间的共用接口；

考虑到需要协同工作，努力制定有效和协调的全球~~框架来应对~~航空网络安全框架，~~和支助~~以协调一致的方式防止和抵御这个部门受到~~全球航空系统网络安全和网络复原力，应对可能会带来民用航空安全和/或安保危险的~~网络威胁和风险；

认识到国际民航组织在航空网络安全~~和网络复原力~~方面跨越各个~~不同~~航空学科的领导力和工作；

认识到航空网络安全需要在全球、地区和国家层面进行协调，从而支持~~保证~~防止和抵御措施和程序~~风险管理体系~~的一致性和~~全面~~互操作性；

认识到各国制定和实施明确和全面的航空~~为民航~~网络安全计划~~建立清楚的国家治理和问责制~~的重要性，该计划应涵盖民航网络安全的法律、法规、政策、程序和措施，包括指定负责航空网络安全的国家主管当局与有关国家当局和机构协调，~~和~~

认可旨在协作和整体解决网络安全问题方面相关的规定、指导材料和倡议~~、行动计划、出版物和其他媒体~~的价值~~，~~；和

考虑到 2024 年 8 月 26 日至 9 月 6 日在蒙特利尔举行的第 14 届空中航行会议的成果，以及 2024 年 12 月 11 日在阿曼马斯喀特通过的《关于航空安保和航空网络安全的马斯喀特宣言》的规定。

大会：

1. 敦促成员国通过、~~和~~批准和实施 2010 年《制止与国际民用航空有关的非法行为的公约》《北京公约》和 2010 年《制止非法劫持航空器公约补充议定书》《北京议定书》，将其作为处理民航网络攻击的方法；

2. 呼吁各国和业界利害攸关方采取下述行动来应对针对民航的网络威胁：

a) 实施国际民航组织航空网络安全战略，并利用国际民航组织网络安全行动计划作为工具来支助实施航空网络安全战略；

b) 制定并实施国家航空网络安全计划，涵盖战略航空网络安全目标、治理和职责、政策、通信、网络风险管理、事件响应和恢复、能力建设和培训、法规合规和审计、监测和持续改进、文件和记录保存，目的是以整体方式应对所有航空学科面临的民航网络威胁和风险；

c) 制定并实施支持航空网络安全计划实施和监测的流程和工具；

d) ~~b)~~作为国家航空网络安全计划的一部分，指定航空网络安全主管当局，并确定该当局和相关国家航空和非航空部门之间的互动；

e) ~~c)~~ 确定国家机构和业界利害攸关方在民航网络安全方面的责任；

f) 得到足够的资源，确保具备和持续培训合格和称职的航空和网络安全专业人员，他们能够监管、操作、管理、维护和监督相关航空网络安全法律、法规、政策、程序和措施的有效实施；

g) ~~d)~~ 制定和实施强大的网络~~安全~~风险管理框架，将网络风险管理整合到~~吸取相应~~相关的安全、~~和~~安保、效率和能力风险管理做法，和采纳基于风险的方法，来加强防止和抵御~~保护~~重要的民航数据、信息和系统~~、信息和数据免受~~受到网络威胁和风险；

h) ~~e)~~ 酌情制定法律、法规、政策、程序和措施~~和~~并分配适当资源来确保，针对关键的航空系统：系统架构在设计上是安全的；系统受到保护并具有韧性；数据在存储和在使用及迁移时安全并可用；系统监测和网络事件检测和报告以及方法得以执行；网络事件响应和恢复计划配合既定的紧急响应和危机管理计划得到开发和实施；以及进行网络事件的法医分析；

i) ~~设计并实施~~制定和实施实际行动，以加强~~跨民用航空领域~~跨所有民航实体的网络安全文化；

~~f) 鼓励政府/业界针对航空网络安全战略、政策和规划以及信息共享进行协调，从而帮助确定需要解决的关键漏洞；~~

j) ~~h)~~ 在国内和国际范围建立并参与政府/政府和政府/行业之间的伙伴关系和机制，系统地共享有关网络威胁、事件、漏洞、危害指标、趋势、~~和~~缓解措施、最佳做法和经验教训的信息；

k) g) ~~鼓励民用/军方~~与相关国家实体，包括但不限于军事、执法和网络安全部门，建立合作机制，以识别、保护和监测~~民用和军事航空系统接口~~可能影响民用航空系统的常见漏洞和~~数据~~信息流，并合作缓解和防范~~响应~~常见的网络威胁，以及应对网络事件和从中恢复~~网络事件~~；

~~a. 鼓励各国继续为国际民航组织在制定国际标准、战略和最佳做法时做出贡献，以支持推进航空网络安全和网络复原力，和~~

l) ~~k)~~ 根据平行、跨部门和功能性的方法，继续协作和促进制定国际民航组织的航空网络安全框架，涵盖~~航空安全、航空安保、简化手续、空中航行、通信、监视、空中交通管理、航空器运行、适航性、以及其他~~所有相关航空学科，以便全面解决对航空安全、安保、效率和能力的网络威胁和风险。

3. 指示国际民航组织：

a) 继续推动普遍通过和批准2010年《制止与国际民用航空有关的非法行为的公约》（北京公约）和2010年《制止非法劫持航空器公约的补充议定书》（北京议定书）；和

b) 继续确保通过~~国际民航组织解决航空网络安全问题的新机制~~国际民航组织所有相关实体之间的协作，以跨领域和整体的方式考虑和协调航空网络安全~~和网络复原力~~问题。

— 完 —