国 际 民 用 航 空 组 织

工 作 文 件

A39-WP/99
EX/45，TE/26
27/7/16
第 1 号修改稿
（Revision No. 1）

大会 — 第39届会议

执行委员会
技术委员会

议程项目16：航空安保
议程项目36：航空安全和空中航行实施支助

民用航空的网络抵御能力

（由美国、及由斯洛伐克代表欧洲联盟及其成员国[1]、欧洲民用航空会议的其它成员国[2]和欧洲空中航行安全组织提交）

执行摘要

民用航空系统由相互连接的要素、系统和网络镶拼组成。在过去几年，对不同航空利害攸关方之间的通信和信息交流造成破坏、影响安全和安保、并损及航空商业持续性的网络事件发生可能性已经增加。国际民航组织虽已认识到为民用航空定义一套适当网络安保做法的重要性，但仍需要额外努力以便提高全球意识，并进一步为航空系统制定全球协调的有关网络抵御能力的做法。

行动：请大会：

a) 要求国际民航组织以全面的方式处理民用航空网络抵御能力；
b) 要求国际民航组织及其缔约国促进对民用航空网络威胁和脆弱性的认识，特别就系统设计、空中交通管理程序和安全管理与航空安保等相关进程和活动，在其中纳入网络抵御能力的考虑因素；
c) 要求国际民航组织以安全的方式促进各国和相关利害攸关方之间就网络威胁、脆弱性和缓解措施等交流信息；
d) 要求国际民航组织考虑必要步骤，从查明到缓解目前和未来网络威胁与脆弱性，制定管理指导原则，并将相关现行国家措施和业界标准纳入考虑；和
e) 要求国际民航组织指示现有专家组和专家小组在进行其工作时，酌情考虑到这些指导。

战略目标：	本工作文件涉及安全、空中航行能力和效率、安保和简化手续等战略目标。

[1] 奥地利、比利时、保加利亚、克罗地亚、塞浦路斯、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、爱尔兰、意大利、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、波兰、葡萄牙、罗马尼亚、斯洛伐克、斯洛文尼亚、西班牙、瑞典和联合王国

[2] 阿尔巴尼亚、亚美尼亚、阿塞拜疆、波斯尼亚和黑塞哥维那、格鲁吉亚、冰岛、摩尔多瓦共和国、摩纳哥、黑山、挪威、圣马力诺、塞尔维亚、瑞士、前南斯拉夫马其顿共和国、土耳其和乌克兰

财务影响：	所附大会文件提及的活动将视2017年-2019年经常方案预算可用资源和/或预算外捐助而进行。
参考文件：	Doc 10022 号文件：《大会有效决议》（截至 2013 年 10 月 4 日） 附件 17 — 《安保 — 保护国际民用航空免遭非法干扰行为》

1. 引言

1.1 航空系统由相互连接的要素、系统和网络镶拼而成。新的发展趋势如遥控驾驶航空器系统(RPAS)的渐进出台和空中交通管理系统(ATM)(如全系统信息管理(SWIM))的持续演进等，更加强化了这种系统互连性和整合。虽有迄今已采取的预防性安保措施，但航空系统受到网络事件影响的风险已然增加。

1.2 在全球一级已认识到适当航空网络安保做法的重要性。但是，仍有必要提高全球意识和进一步为航空系统制定全球连贯的有关网络抵御能力的做法。

1.3 网络事件可在许多层面上影响全球航空界或个别系统。这些事件会破坏不同航空利害攸关方之间的通信和信息交流、影响安全和安保、并有损航空商业持续性。共享网络相关信息和应用强有力的标准方法以保护数据和信息交流的能力，将能提高航空界自我保护和限制网络事件影响的能力。

2. 讨论

2.1 虽然在地方、国家、地区和全球各级均已制定多项倡议，但若有一套更标准化、一致和连贯的做法，将更能应对多变的航空网络威胁环境带来的风险。

2.2 提高全球对航空网络抵御能力的意识

2.2.1 特定经济部门如银行等，既熟知网络威胁和脆弱性，也已为缓解已查明的风险而实施了对抗措施。但是在航空领域，并非所有国家和利害攸关方都对网络相关风险有很好的了解，它们也尚未以一致和系统性的方式对其加以处理。

2.2.2 有必要提高全球航空部门对网络威胁和脆弱性的意识，以确保所有国家和利害攸关方都查明可能出现的风险，并加以缓解。

2.2.3 这种意识加强若要特别正式化，可藉由调整现有进程如通过制定结合安保的设计做法、或实施专门培训而加以实现。此外，经与安保相关倡议协调(若有的话，如安保管理体系、或是国家民用安保方案)，可在组织一级(在其安全管理体系— SMS 之内)以及国家或地区一级(在国家安全方案 — SSP 之内)的安全管理活动、和酌情在地区航空安全方案等背景下，将网络抵御能力纳入考虑。

2.3 促进网络事件、威胁和标准化做法等方面的信息交流

2.3.1 没有任何组织或利害攸关方集团能够独力保护自己免遭未授权的蓄意电子干扰。还有，网络威胁千变万化，没有任何人能假装不受任何相关可能风险影响。要有效应对网络事件，各国和利害攸关方就必须共享相关信息，协调该如何保护和维护数据完好性和信息交流。信息共享可帮助各国和利害攸关方更好地准备应对网络事件，并采取适当行动加以缓解。共享的信息可包括事件的发生、脆弱性、威胁、趋势和已观察到的模式、对共享风险的评估、风险处理计划、成功的缓解手段(技术、运行或组织)、或已验证提供有效保护的安保保障活动。

2.3.2 航空界已有多项促进安保相关(经常是敏感性)信息交流的倡议，包括在地区和全球一级的交流，但这方面的工作仍有待进一步发展和加强，以支持整体航空系统的网络抵御能力。此种倡议可以现有信息共享平台如 ISAC(信息共享和分析中心)或 CERT(计算机应急团队)为基础，可能需要建立关于网络事件信息共享的共同程序，以遵守国家和地区的敏感信息保护规则。

2.3.3 还有必要就数据及所有相关利害攸关方之间的交流信息加强保护方法。应鼓励进行技术管制标准化，从而为全球航空界提供更强有力的鉴别和数据授权方法。

2.4 推广“联合航空风险管理做法”

2.4.1 航空风险评估方法繁多，其中许多均侧重于对威胁和脆弱性测定特性和进行评价。虽然各方可能就测定风险特性的必要因素意见相同(如发生的可能性和影响规模等)，但在具体详细情况评估方面仍众说纷纭，难以有具可比性、相干甚或连贯的结果。不过，面对可能具有类似模式并重复发生的网络事件时，定义一套“共同原则”和查明、评估和缓解风险的方法会有好处。

2.4.2 此种“共同原则”应可促进查明威胁和脆弱性、得以评估风险、并提供缓解工具。对进行风险评估背景加以说明的安保范围正式定义即为一例，正如国际民航组织附件 17 现行规定所预见，此一范围的定义有助于查明关键的航空信息系统。另一个例子就是考虑端对端的“威胁设想”，其中涵盖了威胁、所审查的系统架构、以及导致发生不利影响的资产等。在威胁设想内也包括已知的脆弱性，并可能需要有与影响严重程度相当的缓解办法。

2.4.3 一旦界定和通过了航空风险评估“共同原则”，在理想情况下，还可在国际民航组织制定或修订标准和建议措施(SARPs)的框架中加以适用。

—完—