国 际 民 用 航 空 组 织

工 作 文 件

A41-WP/74
EX/36
26/7/22

大会 — 第41届会议

执行委员会

议程项目14：航空安保 — 政策

制定一个网络安保框架

（由捷克代表欧盟及其成员国[1]、欧洲民用航空会议的其他成员国[2]、非洲民用航空委员会的成员国[3]、和EUROCONTROL提交）

执行摘要

随着新技术和航空更多依赖信息技术和数字运营系统造成新的脆弱性和新机会，网络安保愈发重要。对网络领域更深入的了解进一步指向若干具体挑战，凸显需要推动采取独特的方法来缓解风险并取得进展。其日益增长的重要性进一步强调迫切需要各国和国际民航组织加紧努力，支持制定网络安保框架及网络安保文化和培训。

1 奥地利、比利时、保加利亚、克罗地亚、塞浦路斯、捷克、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、西班牙和瑞典。

2 阿尔巴尼亚、亚美尼亚、阿塞拜疆、波黑、格鲁吉亚、冰岛、摩尔多瓦共和国、摩纳哥、黑山、北马其顿、挪威、圣马力诺、塞尔维亚、瑞士、土耳其、乌克兰和联合王国。

3 阿尔及利亚、安哥拉、贝宁、博茨瓦纳、布基纳法索、布隆迪、喀麦隆、佛得角、中非共和国、乍得、科摩罗、刚果、科特迪瓦、刚果民主共和国、吉布提、埃及、赤道几内亚、厄立特里亚、斯威士兰、 埃塞俄比亚、加蓬、冈比亚、加纳、几内亚、几内亚比绍、肯尼亚、莱索托、利比里亚、利比亚、马达加斯加、马拉维、马里、毛里塔尼亚、毛里求斯、摩洛哥、莫桑比克、纳米比亚、尼日尔、尼日利亚、卢旺达、圣多美和普林西比、塞内加尔 、塞舌尔、塞拉利昂、索马里、南非、南苏丹、苏丹、多哥、突尼斯、乌干达、坦桑尼亚联合共和国、赞比亚和津巴布韦。

行动：请大会： a) 要求国际民航组织考虑采取必要步骤，推进关于评估航空网络安保风险的指导，同时虑及所涉及的行为方、采取全局跨领域视角的必要性以及本工作文件中描述的独特因素； b) 要求国际民航组织完成对相关现行标准和建议措施(SARPs)和其他国际法律基础的汇编，各国和组织可以此为基础将网络风险纳入其航空框架； c) 要求国际民航组织及其缔约国加强努力，推动专门的网络安保文化和活动，以支持开发足够的人力资源和能力来管理民用航空的网络安保和网络复原力；和 d) 要求国际民航组织考虑在全球和地区一级组织网络安保演习。	
战略目标：	本工作文件涉及安保和简化手续的战略目标。
财务影响：	
参考文件：	

1. 引言

1.1 国际民航组织大会第40届会议通过了A40-10号大会决议 — 处理民用航空网络安保问题。该决议通过横向、跨领域和功能性做法处理网络安保问题，重申保护民航关键基础设施系统和数据免受网络威胁的重要性和紧迫性，并呼吁各国实施国际民航组织航空网络安保战略(2019年10月)。该战略通过网络安保行动计划(CyAP)实施，并得到新成立的网络安保专家组的支持，该专家组将以秘书处网络安保研究组的工作为基础。

1.2 随着数字化对经济产生深远影响并重塑航空部门，网络安保问题变得越来越至关重要。在COVID-19大流行恢复阶段，网络安保也继续对所有部门构成挑战。企业正在更多采用虚拟工作方式，这可能会使他们更易受到网络威胁。这要求考虑到网络安保的具体特点，加紧开发网络安保框架。

2. 网络安保情景为界定风险管理做法展现了独特的要素

2.1 网络安保领域展现出独特的威胁情景。它不仅必须关注寻求直接袭击和大规模伤亡的恐怖主义团体，还必须关注各种各样的其他可能行动方和动机。这可能包括大型有组织的实体、活跃分子和黑客罪犯，他们寻求例如扰乱、胁迫、展示实力、媒体关注或经济利益。攻击也可能无意或有意地影响到民航，甚至可能危及安全，并直接或间接影响该行业。

2.2 网络风险管理中需要考虑的其他要素包括为航空系统提供非航空特定服务的提供商数量庞大，并且他们可能对网络安保需求和风险有不同的理解。

2.3 网络领域的另一个特点是国家监管可能跨部门运行，没有专门针对航空的内容。

2.4 以上情况指向需要界定一种特定的网络安保风险评估做法，其中：

a) 所需的专业知识，特别是与脆弱性和缓解措施相关的专业知识，必须将航空和IT知识和经验结合起来；

b) 需要明确界定评估的范围，重点关注跨越个体运营人/实体和各领域的关键功能的安全、安保和复原力；和

c) 风险评估可以从(全球)信息安保的角度查明潜在的单一故障点，以便适当地予以处理。

3. 制定一个虑及具体情况的网络安保框架

3.1 在制定网络安保框架时，航空部门必须制定不仅跨越航空领域的传统边界的做法(例如既需要宏观视角(例如ATM)也需要个体飞行视角)，还要考虑到非航空部门的不同定位和横向(非具体针对航空)的国家监管，如上文2.2和2.3所述。必须确保一致性，并避免重复、空白以及对国家和运营人实施网络安保框架造成不必要的监管或监督负担。

3.2 航空部门处于有利地位，可受益于并利用现有的国际航空职能、责任和程序。国际民航组织航空安保和安全的标准和建议措施提供了一个坚实的基础，可以在政府和机构层面以此为基础开展进一步工作。信息共享和报告机制也是如此。另外，现有的国际航空法文书将危害安全的行为定为刑事犯罪，应尽可能使用这些文书。

3.3 鼓励各国和各组织审查和考虑相关的国际民航组织网络安保文件并实施现有的网络安保相关标准和建议措施。同样重要的是，各国和各组织从数字角度重新思考现有的航空安保和安全，以及航空刑法的结构，以确保各职能和责任与时俱进并适当协调一致。

4. 网络安保中人的因素之关键性

4.1 正如国际民航组织航空网络安保战略（2019年）所认可，人的因素是网络安保的核心。

4.2 航空系统日益数字化和相互连通要求加紧努力，以满足对提高认识、培训、更新学术课程以及得到适当培训、具有航空和网络安保跨领域专业知识的工作人员日益增长的需求并对此提供支持。

4.3 国际民航组织秘书处启动了首期国际民航组织网络安保和网络复原力课程，“航空网络安保领导力和技术管理基础”，以及与EUROCONTROL合作开发的“在ATM中管理安保风险”课程。在这些广受欢迎的努力和吸取的经验教训基础上再接再厉很重要。

4.4 正如国际民航组织航空网络安保战略中所指出，网络安保演习是测试现有网络复原力和查明哪些领域需要改进的有益手段，因此高度鼓励开展这种演习。除了在个别欧洲国家一级进行演习外，欧洲还可以分享在这一领域的地区经验，使国际航空界从中受益[4]。鼓励国际民航组织探索举办此类演习的可能性。

4.5 正如国际民航组织安保文化年（YOSC）期间所强调，将安保和安全文化的概念扩展到实体领域之外至关重要。鼓励各国和各组织在安保文化年的成就基础上继续推广网络安保文化，并分享最佳做法。国际民航组织应推动为此目的的各项努力，包括制定适当的指导材料。

— 完 —

[4] 由欧盟网络和信息安保局（ENISA）组织的“网络欧洲2018”的目标受众包括参与航空领域信息安保活动的专业人士和组织；由于对监视追踪软件的一次网络攻击，欧洲航空危机协调小组（EACCC）在2018年组织了一次危机管理演习，并准备在 2022 年进行一次危机管理演习，模拟欧洲数字网络基础设施由于网络攻击而大规模中断的情景；欧盟航空安全局也组织了网络安保演习。