



第二次高级别航空安保会议 (HLCAS/2)

2018 年 11 月 29 日至 30 日，蒙特利尔

议程项目2：未来管理航空安保风险的方法

制定全球网络安全战略

(由罗马尼亚提交)

摘要

本文件提出了对各国和业界应积极支持制定民用航空全球网络安全战略的建议。

高级别航空安保会议的行动在第4段。

1. 引言

1.1 2018 年 5 月 7 日至 9 日在罗马尼亚布加勒斯特举行了欧洲、中东和非洲 (EMEA) 民用航空网络安全峰会。来自六十五个成员国和十九个国际组织的 416 名代表出席了本次峰会。峰会讨论了如何统一和促进网络安全框架。

1.2 峰会回顾了于 2017 年 4 月 5 日在迪拜首次提出的关于民用航空网络安全的迪拜宣言。此外，会议认可国际民航组织秘书处网络安全研究组 (SSGC) 的工作及其正在进行的工作，力求解决国际航空框架中可能受网络事件影响的所有要素。

2. 讨论

2.1 十年前，网络安全很少作为一个航空业的国际问题受到关注。从当前十年开始，航空专家警告，对民用航空运行的恶意网络攻击可能是灾难性的。随着技术对设计、生产、运行和维护带来剧烈转变，安全和安保模型必须调整适应。

2.2 网络空间已成为经济、社会和政治互动的重要基础。然而，随着相互依赖性和经济机会的增长，也带来了脆弱性和不安全。随着大数据、机器学习和“物联网”的发展，一些专家预计到 2035 年，互联网连接可能增长到近万亿。私人和国家行动者的潜在攻击目标数量将大大扩展，包括从工业控制系统到心脏起搏器、自动驾驶汽车、无人机及尤为重要的民用航空等各领域。

2.3 与其他欢迎“数字革命”的行业类似，航空业必须通过准确地识别脆弱环节和机遇以及了解敌方威胁来维护利益攸关方的信任。以下是相互连接和数字化的民用航空所面临的挑战：

2.3.1 随着航空业越来越多地连接系统和服务，敌方可进行的潜在的系统攻击面越来越大，越来越复杂，导致目标更大。

2.3.2 由于航空业严重依赖技术，并越来越多地依赖网络环境，理解和克服两个行业间的文化差异将需要全球改革。发展共享的文化，共同看待挑战和可能的解决方案需要跨学科合作。

2.3.3 认识到数字力量带来的威胁对于理解和管理风险至关重要。行业中的每个人都必须达到相同的认识和理解水平，以便应对潜在风险并促进重视多角度的协作对话。

2.3.4 航空业在解决安全和安保问题方面有数十年的经验，但网络安全挑战相对较新。与罪犯发展攻击能力相比，开发和更换航空系统可能需要更长的时间，从而对准确进行风险评估和威胁建模带来挑战。

2.3.5 投资于空中交通管理(ATM)已经产生红利，但使用诸如全球定位系统(GPS)、数字通信和自动相关监视 — 广播(ADS-B)等先进技术意味着我们必须管理由于这些技术带来的易受攻击性并鼓励网络抵御能力。

2.3.6 机场是几个不同组织的联合体，各自可能有不同做法，其中一个组织网络易受攻击可能影响所有其他各方。在机场适当保护物理安保系统免受网络威胁至关重要。

2.3.7 关于安全和物理安保已商定国家和国际政策和法规并达成谅解，但目前尚不清楚航空网络安全如何能够实现同样的成熟度和清晰度。鉴于此，国际民航组织、欧洲航空安全组织、欧洲空中航行安全组织、欧洲民航组织以及其他多边实体必须在共享、跨职能和跨边界的网络环境下，并肩制定政策和法规，统一系统思路、治理和问责制，建立有抵御能力的相互信任和得到安保的人类决策流程。

2.3.8 国际民航组织处于有利地位，可以将众多全球航空网络安全举措汇总并使之统一，发挥领导作用和制定标准。为了促进各国间制定网络安全标准的一致性，并推动不同利益攸关方之间的对话与协作，需要对《芝加哥公约》附件(8,10,17,18等)进行关键的评估，相应地从网络安保的角度予以修改。需要真正认识到，通过网络手段的非法干扰现在已成为现实，且有必要在目前对物理实体的重视中纳入网络视角及众多平行因素。

2.3.9 开发网络安全能力 — 人员、技术和流程之间的协同作用 — 使用基于信息网络的运行做法和能够检测、保护、防御、分析、决定和反应并恢复，将确保民用航空在可预见的未来具有抵御能力。

2.3.10 全面和及时的信息共享可将风险降至最低，此类协作工作带来的增值是可以更好地管理利益攸关方的网络安全。新成立的欧洲航空网络安全中心与欧盟计算机紧急响应队、航空情报共享和分析中心或安保运营中心相连，加倍增强了成员国的网络安全能力。

2.3.11 军民共享信息也很重要。军方如何看待和处理在面临无线电频率恶意占频和欺骗性干扰及网络威胁的环境下保护航空器和系统安全这一挑战，可为民用航空提供经验教训。

2.3.12 欧洲航空安全组织制定了“关于民用航空网络安全高级别工作的布加勒斯特宣言”，重点关注若干目标，例如欧洲层面的协调、国际合作、风险评估、提高认识、信息共享和研究与开发。还希望法规在国际上得到统一，因为挑战需要更广泛的全局性做法。

3. 结论

3.1 考虑到为了制定一个网络安全生命周期，网络风险管理从概念、设计一直延伸至保障、供应、建设、交付、运营和维护；因此，需要一种采取总体、全面和综合的做法。为了弥合现状和预期结果之间的差距，有必要采取行动，尽早应对新网络环境中的风险和威胁。

3.2 参加国际民航组织欧洲、中东和非洲民用航空网络安全峰会的国家、地区和国际组织及业界的官员和代表于 2018 年 5 月 7 日至 9 日在罗马尼亚布加勒斯特召开了会议，以应对国际民用航空面临的网络威胁挑战。

3.3 牢记有必要确保民用航空以有序的方式实现安全、安保和连续性，我们建议：

3.3.1 尽可能以协调一致的方式建立国家和行业网络安全框架；

3.3.2 各国和业界以现有举措为范例，在界定共同战略、交流信息和最佳做法方面促进区域合作；

3.3.3 推动信任框架，以便酌情共享安保情报；

3.3.4 各国和业界开展合作，确定长期的人力资源需求，并制定吸引、教育和留住下一代航空专业人员的战略；和

3.3.5 各国和业界在国际民用航空组织的主导下积极支持制定全球网络安全战略。

4. 高级别会议的行动

4.1 请航空安保高级别会议核准上述结论，并支持需要在网络安全领域采取总体、全面和综合做法。