国 际 民 用 航 空 组 织

工 作 文 件

A39-WP/187[1]
EX/72
10/08/16

大会 — 第 39 届会议

执行委员会

议程项目16：航空安全－政策

网络安全防御策略

（由CANSO提交）

执行摘要

网络安全是民航系统中最重要的问题之一和最热的辩题之一。因为对信息技术的依赖程度越来越高，航空系统的演变导致了安全和连续性影响方面的新风险。空中交通管理(ATM)系统，以及飞机系统、机场管理系统、预订系统、航空信息和天气信息同样可能因网络事件受到影响，这些网络事件不仅涉及保密性，主要还是与可用性和连续性相关。

行动：大会获邀就第5条中所述的建议达成一致。

战略目标：	本工作文件涉及战略目标C－安保和简化手续
财务影响：	降低保险成本；缓解灵活性和安全方面的威胁和危险；以及最大限度降低与风险管理相关的成本和社会影响。
参考文件：	《芝加哥公约》附件17 —《安保》；Doc.8973；Doc.9985；Doc 9854；CANSO网络安全风险评估指南

[1] 中文、英文、阿拉伯文、法文、俄文和西班牙文版本由CANSO提供。

1. 引言

1.1 民用航空是犯罪份子和恐怖份子的潜在首要目标。保护民用航空免遭非法干扰行为侵害需处理复杂的威胁，包括技术威胁。社会总是认为作为整体的航空业没有因为安全漏洞而导致的事故和事件。该观点使得最终客户树立了对航空运输的信心。航空运输网络对全球经济至关重要，亦是国际贸易、旅游业、投资和繁荣的基础。若破坏其效能，则可能导致全球经济和社会遭遇重创。制定能够在全球国际环境中互用的复杂系统，需要能够持续监控资源，实现信息技术(IT)、逻辑安全和人身安全之间的流程整合的安全治理方法策略。为此，应持续评估威胁级别和潜在漏洞，以防止、对抗和应对非法干扰行为。另外，这还需要航空系统、国家和有关利益相关者的所有参与者之间紧密协调。仅仅符合法规还不够，展开针对空中和地面人身安全的尽职调查并确保系统的安全、连续性、灵活性和规律性是始终必要的。ICAO 威胁和风险工作小组(TRWG)还强调，就其信息和通讯复杂度而言，全球航空系统必定是严重网络攻击的潜在目标。互用性目标和针对以网络为中心的运营理念的网络开放(通过实时分享信息和运行数据实现)即针对更多漏洞开放系统。

1.2 ICAO 已经表达了网络安全可能是实施全球空中航行计划(GANP)的绊脚石的担忧之情，还为主要航空业利益相关者提供联合行动计划，以系统地评估现有的网络框架(2014 年 12 月 5 日在蒙特利尔签署了行业高级别小组网络行动计划[IHLG])。

1.3 在 2016 年 3 月举行的 ICAO 航空安全小组会议(AVSECP/27)期间，很多成员国强调应升级并标准化附件 17 —《安保》中关于网络安全的推荐做法。但大多数成员国都认为，网络安全不仅仅限于航空安全系统。成员国强调非常有必要确保适当的协调，包括符合其他附件要求，即附件 3、6、10、11、14 和 15 的要求。另外，还应与其他小组协调，而后再升级并标准化当前的推荐做法，而且还需咨询 ICAO ANC。

1.4 CANSO 想要强调保护航空系统内所有数字信息和系统的重要性。务必应确保保护公众、旅客、机组人员、地面人员、飞机和航空设施免遭地面或空中不法干扰行为的侵害。如 ICAO“不让一个国家落后(NCLB)”行动计划所述，可能需要采取特定的措施在欠发达国家完善该概念。

2. 澄清网络安全的必要性

2.1 CANSO 指出，“网络安全”一词容易让人混淆，它用于表示敌人造成的威胁，以及有必要评估和修复 IT 系统中的漏洞。另外，它还用于描述如何根据灵活性实施有效的应急计划。

2.2 CANSO 强调，有效的民航安全策略不仅要考虑技术成熟水平，主要还是考虑实现基本航空安全目标的保护方法策略。只有通过自下而上的策略才能实现该目标，包括整个组织，且考虑人为因素。

2.3 全球空中交通管理运营理念(ICAO Doc.9854)清楚地讲述了该目标，其中明确描述了安全的重要性并通过非常新颖的方式提出来。

“安全是指防止因故意行为(例如，恐怖主义)或非故意行为(例如，人为错误、自然灾害)影响飞机、人员或地面设施而遭遇威胁的举措。充分安全是空中交通管理(ATM)社群的主要期望。因此 ATM 系统应确保安全，ATM 系统以及与 ATM 相关的信息应加以保护，以免遭安全威胁。

2.4 从这个角度看 — 与 IT 安全主要标准相关，提供可用性、完整性和保密性的目标即缔约国确保根据《芝加哥公约》尤其是 ICAO 附件 17—《安保》要求保护民航主要构成部分的一般义务。

3. 新方法

3.1 CANSO 强调，对民航安全至关重要的相关资产的保护可能会有所不同，具体视相关航空利益方的目标而定，包括政府、ANSP、航空公司、机场、制造商、军方等。可明确针对所有社群成员的一些航空网络安全主题并按具体需求定义，以便：

a) 确保仅授权人员可访问关键信息，以防止通过内部威胁对运营商的核心服务独立发起非法干扰行为；

b) 根据常识和*善意*履行义务，勤奋谨慎识别和解决关键系统的漏洞；

c) 将风险管理延伸至因更加依赖单一运营商的 IT 资源导致的风险；

d) 落实针对事件处理和危机管理的适当响应管理措施，包括应急计划；

e) 在国家民航安全计划(National Civil Aviation Security Programme)的框架下评估(网络)安全漏洞对单一运营商以及整个行业的影响。

3.2 换句话说，网络安全与传统的航空安全策略不同，它是附件 17(安全)所述基本原则和指导材料(解决最常见的人身安全威胁和漏洞）的自然延伸。

3.3 航空网络威胁将最可能是任何全新现代化计划中的重大安全威胁之一，如单一欧洲天(SES)、SES 空中交通管理研究(SESAR)、下一代(NEXTGEN)以及其他在区域范围内制定的计划。它似乎是航空行业其他部分中最相关的驱动因素之一。作为关键资源，信息必须像任何其他对 ATM 系统的续存和成功至关重要的资产一样加以对待。所有那些计划，不仅仅是 ATM，还涉及飞机运营商、机场、军方和其他，将以全系统信息管理(SWIM)概念为基础，促进信息和服务在整个系统范围内以网络为中心的运营交流。SWIM 将改善协作决策，根据需求在适当的时刻向适当的接收人提供更高质量的所需信息。SWIM 是未来航空技术环境的关键促成因子，其相关基础设施应视为关键基础设施，而该等基础设施的安全应专门视为关键要求。

3.4 就此而言，尽管鉴于国家主权、国防、情报和执法的影响，一般安全是缔约国的义务，但考虑航空环境的特殊性有助于制定更高效的行动。

3.4.1 各区域的相关行动方案正在展开或已实施。列举一下最近的成果：欧盟对 ATM 网络的立场，已在发布的一期《欧盟条令》(Reg. 1035/2011)中明确表明，指出了安全漏洞之间的清晰关系并规定了针对网络安全的约束要求。美国联邦航空管理局(FAA)在提交给参议院的提案中宣布了针对挑战

目标的相关网络安全目标(Sec.4109)，包括一系列应对网络问题的行动。其他国家亦正在以类似的方式在监管层面上专注于航空网络安全方面的工作。

3.4.2 鉴于网络安全对民航的重要性，CANSO 全力支持旨在充分整合国家和地区航空安全计划内网络安全主题的行动计划并宣布完全可积极参与。

4. 结论

4.1 航空网络安全是从方法论和现实角度探讨的主题，考虑对整个行业和公众信心的影响。

4.2 CANSO 推动 ICAO 领导下的全新国际行动计划，以有效和可持续的方式展开，并坚持“不让一个国家落后”的原则。

4.3 在 2014 年 12 月签署网络安全行动计划之后，行业高级别小组(网络)行动计划正在制定改善该领域自愿合作的框架。该行业领导的计划应通过法规认可并更深入地考虑网络安全代表的民航业交叉问题，为其提供补充和支持。

5. 建议

5.1 大会获邀为 ICAO 秘书处紧急分派任务，即以合理、可持续和有效方式，让网络安全实际成为航空安全的一部分。大会获邀对以下建议达成一致：

大会：

a) 考虑并批准文件内容，认可与民航的相关性和可能对其造成的影响；

b) 同意 ICAO 针对作为航空安全内垂直领域的航空网络安全制定全新的策略，并发布以当前区域和国家行动计划和谐化为目标的指导材料；

c) 建议成员国专注于系统和网络中的漏洞而不是威胁，考虑对整个民航业的影响；

d) 建议开设论坛，让航空公司在安全/受信任的环境中分享最佳实践，以分享可改善当前和未来技术产业安全性的高效工具和技术；

e) 建议成员国查看 AVSECP/27 期间提交的近期行动计划，以升级并标准化附件 17 中的当前推荐做法 4.9.1 和 4.9.2；以及

f) 留意CANSO“网络安全和风险评估指南”[1]。

—完—

[1] https://www.canso.org/canso-cyber-security-and-risk-assessment-guide