国 际 民 用 航 空 组 织

工 作 文 件

A42-WP/150
EX/73
29/7/25

大会 — 第 42 届会议

执行委员会

议程项目18：能力发展和实施支助 — 政策和活动

关于制定符合新指南的网络安全培训方案的提案

（由大韩民国提交）

执行摘要

对近期航空网络事件统计数据的分析表明，网络威胁已演变为**现实危险**。为此，网络安全专家组正根据国际民航组织**附件 17《安保》第 4.9 段**，制定并发布相关指南。然而，目前仅有一门正式的国际民航组织网络安全培训课程可供使用。为了建设能力来应对这些现实威胁，就需要进行教育和培训。因此，有必要鼓励成员国根据网络安全指南制定培训方案，并由国际民航组织对这些努力**进行标准化**。

行动：请大会：

a) 认识到针对民用航空的网络威胁不断演变的性质；
b) 审查根据附件 17 —《航空安保》第 4.9 段的要求所制定的网络安全指南；和
c) 启动由国际民航组织牵头、基于这些网络安全指南的新的国际民航组织培训方案的制定工作。

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。
财务影响：	本文件中提及的国际民航组织各项活动预计将按照国际民航组织 2026-2028 年业务计划的指导，在 2026-2028 年经常预算和/或预算外捐助提供的可用资源范围内开展。
参考文件：	Doc 10184 号文件：《大会有效决议》（自 2022 年 10 月 7 日起生效） A42-WP/12 号文件：民用航空网络安全问题 A42-WP/13 号文件：在阿曼马斯喀特举行的国际民航组织 2024 年安保周高级别部长级会议的成果

1. 引言

1.1 最近，网络攻击的目的一直在发生变化。过去，攻击者侧重于窃取旅客姓名、电话号码和信用卡等个人信息。现在，他们的目标正在转向对民用航空造成直接和有形的干扰，例如使航空运输服务瘫痪或使空中航行系统中断。

1.2 根据 EATM-CERT 发布的截至 2025 年上半年的一年间数据，最常见的网络攻击类型是勒索软件，占 33 起事件总数中的 15 起（约 45%），其次是黑客攻击（7 起）和分布式拒绝服务攻击（DDoS，5 起）。主要攻击目标为航空公司，共发生 16 起事件（约占 48%），其次为机场（7 起）、供应链（7 起）和民航局（CAA，3 起）。

1.3 预计此类案件将继续增加，而鉴于未报告的事件数量庞大，必须将网络威胁视为航空业面临的现实且迫在眉睫的危险。

2. 讨论

2.1 国际民用航空组织附件 17（安保）第 4.9 段要求确定用于民用航空用途的重要信息和通信技术系统和数据，并根据风险评估，酌情制定和实施措施，保护其免遭非法干扰行为。

2.2 大韩民国去年通过普遍安保审计计划持续监测做法（USAP-CMA），使其国家网络安全法规符合所要求的相关标准。预计许多成员国也将能够充分满足这些标准。

2.3 此外，网络安全专家组在过去四年中已制定并部分发布了多份指导文件，旨在加强航空网络安全能力，指导成员国更便捷地在民用航空领域应用这些文件。

2.4 从这个角度来看，现在是针对这些指南平行开展国际民航组织培训的适当时机，有必要为正在制定或已经公布的网络安全指南制定教育和培训方案。（国际民航组织培训中目前有一个网络安全培训方案）。

3. 结论

3.1 对过去五年的统计数据和近期数据的分析表明，我们必须认识到，现在是主动强调加强航空网络安全弹性的时候了，因为对民航的网络威胁已经成为现实。

3.2 在网络安全专家组的领导下，正在制定和发布针对附件 17（安保）第 4.9 段建议的网络安全指南。所有成员国需识别这些指南并制定机构调整措施。

3.3 要实现这一目标，最关键的需求是制定网络安全教育和培训方案。尽管网络安全专家组正在制定培训指南，但目前仅有一门正式的国际民航组织培训课程。国际民航组织应鼓励许多成员国开展网络安全培训，并推动其标准化。

— 完 —