国 际 民 用 航 空 组 织

AN-Conf/14-WP/125[1]
29/6/24

工 作 文 件

第十四次空中航行会议

2024 年 8 月 26 日至 9 月 6 日，加拿大，蒙特利尔

议程项目 **4：** 空中航行系统的超联通
4.2： 网络安全和信息系统的韧性

关于提供空中交通服务（ATS）的网络安全问题

（由阿根廷提交，并得到拉丁美洲民航委员会（LACAC）[2] 19 个成员支持）

执行摘要

本文件就设计一套机制以支持空中交通服务（ATS）提供者管理网络威胁和网络事件以及制定有效缓解策略提出了一些想法。

行动：请会议：

a) 制定指导机制，协助空中交通服务提供者在其安全管理体系中管理与安全相关的网络风险；

b) 开发和/或实施技术、程序和安排，使管制员能够安全地提供空中交通服务（ATS），并在发生网络事件时迅速恢复运行；和

c) 确定空中交通管制员所需的能力和技能，以便评估和应对网络事件及其对提供空中交通服务的影响，从而实现网络韧性。

1. 引言

1.1 鉴于航空业网络威胁和网络攻击频增，并忆及国际民航组织航空网络安全战略和基本网络安全政策的七大支柱之一是将网络安全纳入航空风险管理，尽管事实上空中航行新兴技术正在不断发展以更好地处理网络事件，但识别和衡量此类事件对空中交通服务（ATS）提供的影响比以往任何时候都更为重要。

[1] 西文版由阿根廷提供。

[2] 阿鲁巴（荷兰王国）、伯利兹、智利、哥伦比亚、哥斯达黎加、古巴、多米尼加共和国、厄瓜多尔、萨尔瓦多、危地马拉、洪都拉斯、牙买加、墨西哥、尼加拉瓜、巴拿马、巴拉圭、秘鲁、乌拉圭、委内瑞拉玻利瓦尔共和国。

1.2 由于航空系统彼此之间以及与其他外部系统之间错综复杂地联系在一起，网络事件的影响范围和影响力越来越大，有可能引发全球性中断事件[3]。因此，重要的是将网络事件视为安全危险源，或至少视为《2023-2025 年全球航空安全计划》（Doc 10004 号文件，GASP）中所述的全球高风险类别（G-HRC）事件的前兆和促成因素。此外，《空中交通管理运行概念》（Doc 9854）警告说，决策往往基于不同的标准，包括安全标准。这种情况要求采取行动，以实现 Doc 9854 附录 E 中提到的预期效益之一：[…] 扩大危险源的界定范围将能够为用户提供更稳定的航迹。

1.3 空中交通服务在更加自动化、数字化和互联的环境中提供，使其更容易受到网络威胁和网络攻击。管制员-驾驶员数据链通信（CPDLC）的使用、将无人航空器纳入管制空域、远程数字塔台和机场自动飞行信息系统（A-AFIS）等新的发展情况证明需要提高意识和采取行动应对网络事件对提供空中交通服务的影响。

1.4 在预防和/或减轻网络事件方面确实取得了重大进展。然而，根据定义，此类事件直接涉及空中交通管理/通信、导航和监视（ATM/CNS）和信息系统，因此需要开展更多工作来紧急应对网络事件对空中交通管理的影响。

1.5 如果空中交通服务单位没有建立足够的风险控制和防御屏障，可能会出现部分服务中断、零空中交通管制（ATC）状况，甚至发生如飞行中航空器失去间隔的安全征候事件，从而可能导致全球五大高风险事件类别之一的空中相撞（MAC）。

1.6 国际民航组织秘书处网络安全研究组（SSGC）制定的网络安全行动计划（CyAP）第 4 节 — 制定网络安全政策提出了管理网络风险的行动。在此基础上，值得重新思考在全球背景下作为空中交通服务的一部分对安全风险的管理方式，这种方式据述为不稳定、不确定、复杂和模糊，并且越来越脆弱和非线性[4]。

2. 讨论

2.1 鉴于上述情况，必须查明提高预测能力并采取行动的机会，以加强提供空中交通服务的网络安全。

2.2 首先，有必要重新审视提供空中交通服务日益复杂的运行环境，并重新定义空中交通服务单位的作用和职能，特别是在需要采取行动的四个综合管理系统交叉点：网络风险管理、安全风险管理、安保管理和信息安全管理。

2.3 此外，有三个空中交通服务相关方面需要设计和实施网络事件缓解措施：

a) 与提供空中交通服务相关的安全风险管理；

[3] 中断事件：在国家、地区或全球范围内发生、对航空产生不利影响的异常严重事件。此类事件通常不是由航空活动引起的，但仍然会对运行产生重大影响。

[4] 这一描述取自社会科学模型 VUCA（易变、不确定、复杂、模糊）和 BANI（脆弱、焦虑、非线性、难以理解），用于解释当前的全球形势，可应用于所有研究领域。

b) 空中交通服务单位为提供服务所使用的技术/操作工具[5]；和

c) 空中交通管制员（ATCO）在其空中交通服务单位实现网络韧性所需的技能和能力。

2.4 关于空中交通服务安全风险管理，网络威胁和网络攻击应纳入空中交通服务提供者（ATSP）的安全管理体系（SMS）。安全管理体系的第2部分自然具有特别重要的意义，因为从逻辑上必须确认危险源，才能管理相关风险。因此，要从根本上了解，必须对网络威胁和网络攻击如此确认，作为记录其发生、衡量其对空中交通服务影响和评估其风险的第一步。

2.5 这种方法不应仅限于确认传统上与空中交通服务相关的危险源，还应扩展涵盖与信息技术（IT）相关的危险源，例如支持空中交通服务单位的ATM/CNS系统的网络、使用的软件、服务器和硬件以及其他相关要素。随着技术的突飞猛进，这种方法绝对不能被视为静态的，而应被视为动态的和自适应的。这将需要不断修订和调整，以跟上不仅在运行领域而且在整个环境中的快速技术发展。因此，必须认识到，网络事件和征候事件两者都可能演变为空中交通服务提供和飞行运行中的安全事件。

2.6 至于空中交通服务单位使用的操作工具，这些工具被理解为管制员所需的技术、程序和安排，以便安全地提供空中交通服务，并在发生网络事件时实现网络韧性和迅速恢复运行。因此，制定机制以协助管制员快速识别网络威胁并采取适当行动至关重要。

2.7 空中交通管制员的角色已经发生改变，他们与SHELL模型元素的互动方式也随着新常态而发生变化。人、硬件和软件之间的共生关系已益发强化，受到网络事件影响的程度也随之增加。因此，必须培养必要的能力和技能，以便空中交通服务部门的管制员能够实现网络韧性，并能够处理不同的网络事件情景。

3. 结论

3.1 鉴于上述情况，并考虑到网络安全在空中交通服务提供中的跨领域性质，需要有机制为空中交通服务提供者提供指导，将网络威胁和网络事件管理纳入其安全管理体系，并获得设计缓解策略和早期侦测程序的分析工具，以及帮助管制员针对网络事件立即做出决策的工具。

3.2 为使空中交通管制员能够评估和应对可能影响空中交通服务提供的网络安全事件，并增强对可能后果和所涉及的人的因素的情景感知，就此确定空中交通管制员的能力和技能也是恰当的。

3.3 请会议考虑：

a) 制定指导机制，协助空中交通服务提供者将安全相关网络风险作为其安全管理体系的一部分进行管理；

b) 开发和/或实施技术、程序和安排，使管制员能够安全地提供空中交通服务（ATS），并在发生网络事件时迅速恢复运行；和

[5] 这些包括运行程序、计算机系统和其他信通技术、空中交通服务监测、通信等。

c) 确定空中交通管制员所需的能力和技能，以便评估和应对网络事件及其对提供空中交通服务的影响，从而实现网络韧性。

— 完 —