国 际 民 用 航 空 组 织

工 作 文 件

AN-Conf/14-WP/124[1]
29/6/24

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

空中交通服务（ATS）网络安全监管指南

（由阿根廷提交，并由拉丁美洲民航委员会（LACAC）[2]19个成员共同提案）

执行摘要

本文件提出了协调空中交通服务（ATS）监管规定的考虑因素，旨在纳入与可能针对空中交通服务的恶意软件攻击情景有关的规范、方法和程序，以确保对人员的初训和复训进行持续监测。

行动：请会议：

a) 支持本工作文件中提出的举措，同时要求分析将空中交通服务网络安全法规和方法纳入全球航空框架的效用；和

b) 鼓励各国将其国家网络安全战略与国际民航组织民航战略相结合，以建立空中交通服务的网络安全文化，通过制定拟议的监管规定，结合政策、战略和机制作为保障措施。

1. 引言

1.1 民用航空越来越多地使用最先进的全球互联技术，导致了网络威胁风险显著增加。

1.2 国际民用航空组织（ICAO）大会第 41 届会议认识到这一问题的重要性，在《大会有效决议》（截至 2022 年 10 月 7 日）（Doc 10184 号文件）第 VII 部分 — 非法干扰；有关非法干扰的其他事项中纳入了大会 A41-19 号决议：解决民用航空网络安全问题。它呼吁各国采取多项行动；其中一些行动应使用监管工具来处理，从而应对航空界目前的关切，即现有标准、程序和流程是否能将风险在数字连接的环境中有效维持在可接受的水平。

---

[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。

1.3 根据安联集团 2019 年发表的一篇题为“风险晴雨表：最大的商业风险”的文章（引用自《全球空中航行计划》第七版（GANP，Doc 9750 号文件）），最可怕的业务中断（BI）类型是勒索软件网络攻击。[3]WannaCry 和 Petya 是用于攻击欧盟数字系统的两例勒索软件。然而，值得一提的是，文章提到 12%的网络业务中断是由犯罪分子网络攻击造成，而 88%则是由于人与系统交互导致的技术故障或错误而引起。

1.4 所有民航利益攸关方都做出了巨大的合作努力，以保护和保障空中航行系统免遭非法干扰行为，并将风险管理和系统网络韧性作为优先事项。在此背景下，民航监管机构发挥的基础性作用应不断演变。也就是说，除了现行法规外，宜于提供可扩展的灵活创新，特别是考虑到正在发展、重点应是企业对企业和/或企业对消费者[4]的新业务模式。因此，规章条例应规定的是在这一新背景下所需的绩效标准，而不是承袭过去的作用而对技术组成要素个别地具体详细规定。

1.5 因此，监管应促进和推动创新，满足绩效要求，支持空中航行系统的发展，同时确保监测和监督。从这一角度来看，新的监管模式在许多方面代表着从仅为两个行为者（国家监管机构和空中航行服务提供者（ANSP））设计的集中式系统过渡到分布式协调监管系统，而后者可提供适应网络韧性基础设施需求以及用户明确需求的服务。

2. 讨论

2.1 有鉴于此，我们提出了一些考虑因素，以促进统一和协调空中交通服务监管规定。我们的目的是分析有关纳入相关规范和程序处理针对信息系统可能进行恶意软件攻击的情景这一提案，同时满足所有相关利益攸关方的需求，并对初训和复训进行持续监督，以确保人员保持必要的技能。

2.1.1 针对民用航空网络攻击的情景，根据大会 A41-19 号决议：“解决民用航空网络安全问题”并因其犯罪性质而被归类为非法干扰。

2.1.2 技术进步和空中航行系统互联均以安全为目的，但它们可能创造条件，使非法干扰不仅影响航空器，而且影响空中交通服务附属系统。

2.1.3 附件 11 —《空中交通服务》的标准和建议措施（SARPs）以及《空中航行服务程序 — 空中交通管理》（PANS-ATM，Doc 4444 号文件）中规定的方法，是在非法干扰针对航空器或疑似针对航空器的情况下，通过行动或程序来识别。

2.1.4 上述文件均未处理针对空中交通服务附属系统的潜在攻击。因此，可能有必要纳入国际民航组织监管或技术指南来处理受网络攻击影响的空中交通服务附属系统，以便提供适当应对此类事件的充分程序。我们建议研究空中交通服务的非法干扰情景，以便制定反制网络攻击的具体措施。

---

[3] 勒索软件是一种恶意软件，它会加密用户的档案，然后索要赎金才能恢复。

[4] 全球空中航行计划 — 在线。新兴、全新和适应性的商业模式，国际民航组织：https://www4.icao.int/ganpportal/GanpDocument#/lessons/WWfUWzbjlhwCVRRkMTd9NRWaFjpHfZxp

2.1.5 有鉴于此，并根据国际民航组织《网络安全行动计划》，我们建议，分析是否可以纳入关于通知国家指定主管当局的规范和/或程序，以便在怀疑或确认对空中交通服务附属系统的网络攻击时，使所有相关利益攸关方，特别是航空运营人，能够及时交流相关信息。

2.1.6 此外，我们认为，建立军事当局和空中交通服务之间的网络安全信息交换机制至关重要，以便共享相关信息。这种合作方式将有助于减轻空中交通服务遭受网络攻击的风险。

2.2 此外，鉴于《网络安全行动计划》指出需要“在全球、地区和国家层面推行监管协调，以促进全球一致性并确保保护措施的互用性”[5]，我们注意到有必要纳入具体监管规定，但不影响与该问题相关的其他规定的通过，包括：

a) 在地区层面应对网络威胁和网络攻击情景的程序，因为这将为一些国家独力处理面对的经济和技术差异提供应对之道，特别是考虑到网络攻击或网络威胁的影响通常超越国界；

b) 提供足够的工具，将国家网络安全战略与《航空网络安全战略》所载的国际民航组织准则挂钩，从而确保国内民用航空为政策、战略、培训和实施此类战略相关的费用做好安排。还包括指定民航网络安全主管部门，并表明该主管部门将如何与国家组织和其他相关利益攸关方互动;

c) 关于国家空中航行系统安保的规定，以便有架构确保其完好性和保护。可包括就针对民用航空的网络事件进行报告、监督和法证分析[6]的方法；

d) 制定培训规定，以推广空中交通服务的网络安全文化，并为空中航行系统的所有参与人员提供充分的培训。在这方面，为上述人员的培训项目做好安排至关重要；

e) 制定具体的空中交通服务应急措施，以处理这些情况并确保快速恢复运行，包括网络事件的恢复行动和查明关键利益攸关方，以便在危机期间进行有效的沟通和协调；和

f) 制定关于侦测和通知网络事件的规程，建立明确的程序，以便尽早发现和及时通知影响空中交通服务附属系统的任何网络安全事件。这将确保对任何威胁做出快速和协调的反应，从而减少网络攻击对飞行运行安全和连续性的潜在影响。

3. 结论

3.1 空中交通服务的网络安全问题隐患需要在国家、地区和全球层面采取协调行动。采纳了本文件所载建议，就代表朝着加强服务安全性和减轻空中交通服务附属系统网络攻击相关风险迈出了重要一步。通过采用这些方法，各国将更好地准备应对新出现的网络安全挑战，同时确保飞行运行的连续性和完好性。此外，国际合作和监管协调将有助于促进全球航空界建立强大而有韧性的网络安全文化。

---

[5] 《网络安全行动计划》，第 3 章，战略行动计划，支柱 1：国际合作，国际民航组织，2022 版。

[6] 法证网络安全分析是一门用于调查和分析信息安全事件的学科。这些事件包括网络攻击、数据盗窃和入侵。

3.2 因此，请会议批准以下措施：

a) 支持本工作文件中提出的举措，同时要求分析将空中交通服务（ATS）的网络安全法规和方法纳入全球航空框架的效用；和

b) 鼓励各国将其国家网络安全战略与国际民航组织的民航战略相结合，以在空中交通服务中建立网络安全文化，通过制定拟议的监管规定，将政策、战略和机制作为保障措施。

— 完 —