



大会 — 第 42 届会议

执行委员会

议程项目 13：航空安保 — 政策

加强对民航领域数字与网络安全威胁的治理与管理

（由航空航天工业协会国际协调委员会（ICCAIA）和
航空公司飞行员协会国际联合会（IFALPA）提交）

执行摘要

民航业日益依赖互联数字技术和系统，其中包括直接控制或影响物理和运营流程的技术和系统。尽管这些技术具有显著优势，但它们也使整个行业暴露于人为、非人为或自然产生的数字威胁之下，伴随这些技术的漏洞还可能进一步放大这些威胁，危及关键运营环节。

大多数 ICAO 框架（无论涉及安全、安保还是运营领域）在最初设计时，并未考虑到数字威胁的系统性特征和跨域性质，而这些威胁如今已广泛存在于新兴数字功能及其相互依赖关系中。当前最紧迫的缺口在于那些跨越安保与安全边界的故意和恶意行为。

本文件提请 ICAO 首先建立一个内部协调的数字威胁治理与管理框架，为安全、安保和运营领域统一框架，并优先聚焦于故意和恶意威胁。作为补充措施，文件鼓励 ICAO 加快制定必要的指引和全球标准，以在整个航空业生态中实现统一有效的安全保障系统。

行动：请大会：

- 承认所有类型的数字威胁（无论是故意、非故意，还是自然产生）都对民航构成风险，必须通过全面的治理方式加以应对；而这种治理方式应首先由 ICAO 建立，从而为各成员国和行业提供统一有效的支持。
- 请求 ICAO 理事会启动建立 ICAO 内部多领域、多学科数字威胁治理框架的工作。
- 鼓励 ICAO 加快制定相关指引，并在适当情况下制定标准和建议措施（SARP），为所有国家和利益相关方建立系统性、协调统一、可适应变化的数字安全基准；和
- 建议 ICAO 通过其区域网络，加强关于协同应对数字威胁的宣传和沟通，以确保行动协调一致，并提升全球范围内的安全水平。

¹ 英文、阿拉伯文、中文、法文、俄文和西班牙文文本由航空航天工业协会国际协调委员会和航空公司飞行员协会国际联合会提供。

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:	无。
参考文件:	A41-19: 应对民用航空网络安全问题 附件 17 — 航空安保 附件 19 — 安全管理

1. 引言

1.1 数字化转型提升了民航业的运营表现。然而，随着互联性和系统复杂性提升，对数字化技术的依赖不断加深，漏洞逐渐暴露，甚至还可能制造出新漏洞。

1.2 由于涉及 ICAO 各领域（包括安全、安保、运力和效率）之间的职责分担，这一变化给组织和治理带来挑战，凸显了对统一和协调治理更广泛的需求。

1.3 在各类数字威胁中，故意和恶意行为（通常被称为网络安全攻击）亟需优先应对。这些行为可能会干扰关键航空系统，而且当前在安全与安保领域之间职责划分尚不明确。

1.4 这一转变也凸显出目前仍缺乏一个全球性框架，能够为各领域提供专门指引和标准，系统性地实施“设计即安全”和“威胁情报驱动”的方法。在缺乏统一方针的情况下，可能需要建立临时协调机制以支持早期行动，尤其是在高风险的运营情境中。

1.5 “数字威胁”是指源自或经由数字能力促成的任何潜在或实际有害事件，这一概念已开始受到 ICAO 各专家组和工作组的关注。然而，许多此类威胁尚未得到充分关注，尤其是不符合“非法干扰”或“安全隐患”传统定义的数字威胁。对于落入 ICAO 各领域交集的故意和恶意威胁，这种情况尤为突出，从而导致在责任划分、监督机制和协调响应方面存在不确定性。

2. 讨论

2.1 民航业面临的数字威胁形式多样、类型广泛。这些威胁可能是故意的（恶意或非恶意）、非故意的（如人为错误、配置不当）或自然产生的（如环境事件）。它们可能源自数字、物理或混合途径，并影响数字元素及依赖这些元素的物理系统，从而危及航空安全、安保和持续运营。理解这些广泛的威胁类别只是第一步；行业还必须应对持续数字化转型所带来的威胁复杂性加剧的问题。

2.2 数字化转型正在重塑航空生态系统，不仅带来新技术，也引入了新的故障和暴露模式以及依赖关系。许多此类风险未得到传统 ICAO 领域框架的充分覆盖。这首先体现在与安全和安保相关的领域，但远不止于此。全球性结构的缺失导致响应不统一、职责划分不明确和缺乏共识，对航空业的安全与韧性造成影响。

2.3 除了恶意行为风险加大外，组织结构也因数字化转型变得更为复杂，对现有的治理体系和风险/事件管理框架带来了新的挑战。数字化转型导致了信息技术（IT）与运营技术（OT）之间建立起不明晰的相互依赖关系，增加了供应链的风险暴露；同时，技术发展的速度远远快于认证周期所能跟上的节奏。传统航空电子设备如今依赖于云技术、人工智能（AI）和互联网协议（IP）链接，而其中的第三方组件每月更新，持续引入传统控制措施难以覆盖的漏洞。创新以月为单位推进，而监管则以年为周期推动，使得现有缓解措施过时，并加剧了各国之间的差异。由于缺乏统一的分类体系和事件共享机制，行业对问题的认知仅限于零散片段，导致难以及时采取相应防护措施。

2.4 目前缺乏以“设计即安全”和“威胁情报驱动”理念为基础的全球性专门指引与 SARP。意味着在各领域在应对数字威胁时，尚无统一、系统的方法可循。各国缺乏共同的绩效基准，形成了系统层面的脆弱环境，为那些专门利用此类复杂情况的威胁提供了可乘之机。

2.5 在此背景下，故意且恶意的威胁应予以特别重视。这类威胁通常高度复杂、变化频繁且难以溯源，旨在利用数字依赖关系，降低或扰乱航空运营能力。威胁的独特性使其可能会落到传统航空分类体系之内、跨越多个分类，甚至超出这些分类，从而给检测、报告和响应带来挑战。

2.6 实际运营经验表明，某些恶意数字干扰行为在现有各领域框架中并无明确归属。一个典型例子是故意的 GNSS 信号欺骗 — 即通过发送伪造的定位信号来误导飞机的导航系统，且其中不涉及物理接入或可见入侵行为。尽管此类行为属故意行为，可直接影响飞行运作，但它可能不符合《附件 17》对非法干扰的界定标准，也不会触发《附件 19》所规定的强制性安全事件报告。

2.7 这一监管盲区不仅加大了感知与协同响应难度，更凸显出对建立相关治理与管理框架的迫切需求。该框架应考虑这些新型数字干扰形式，设定明确的报告阈值，并清晰界定安全与安保领域之间的机构职责。

2.8 在当前缺乏国际统一框架的情况下，各国和地区监管机构已开始采取多样化的监管做法。不断扩大的差异加大了航空利益相关方（包括整机制造商 OEM、供应商和服务提供商）应对威胁的难度。他们必须面对各国不统一的合规环境。

为应对这一挑战，需采取双重策略：

- 一套全面综合的战略，能够涵盖全部类型的数字威胁，包括故意、非故意，以及自然产生的威胁。
- 同时，也需集中力量，优先应对那些紧迫、潜在影响严重、因当前监管尚未统一而亟待处理的故意和恶意威胁。

3. 结论

3.1 强化对数字威胁的防护，对于保障民航业的安全、安保、运力和效率至关重要。随着各系统和领域对数字技术的依赖日益增强，对具有前瞻性、统一治理的需求也不断增长。

3.2 为应对这一挑战，ICAO 及其利益相关方必须明确实现双重目标：

- 采取综合方法，全面应对所有类型的数字威胁，包括故意、非故意和自然产生的威胁；
- 优先处理故意和恶意威胁，因为这些威胁目前在 ICAO 各相关领域间的职责与协调机制上存在最大的不确定性。

3.3 通过促进各领域协调一致、采取过渡性措施并建立共识，ICAO 能够发挥核心作用，确保各方以协调、灵活且全球统一的方式，应对不断演变的数字威胁。

3.4 这项工作可以由现有的临时网络安全协调委员会（AHCCC）主导，前提是为其赋予明确的治理职责 — 这一职责正是该委员会目前所缺乏的。

— 完 —