国 际 民 用 航 空 组 织

工 作 文 件

A40-WP/395[1]
EX/161
30/7/19
信息文件
(Information Paper)

大会 — 第 40 届会议

执行委员会

议程项目 12：航空安保 — 政策

航空网络安全 — 继续前进

（由国际航空运输协会提交）

执行摘要	
该文件介绍了国际航空运输协会（IATA）认为在了解和管理航空网络安全风险方面需要协调、积极和切实的进展的观点。	
战略目标:	本资料文件涉及战略目标：安全
财务影响:	无
参考文件:	

1. 引言

1.1 航空网络安全（即与维持安全、可靠、适应力强的飞行操作有关的网络安全）仍然是行业的一个关键优先事项。数字化的不断进步和互联性的不断提升正在转变客户可获得的服务，同时使方方面面得到改善，包括提高受监管运营商的效率和可靠性。但这种转变不仅给航空业带来了机遇，也给那些希望造成破坏的人带来了机会。在基础层面上，航空业可以说比许多行业的状况更好，因为航空业注重安全文化、风险和设计的可见性以及针对冗余或故障的培训。但是服务和系统的复杂性和相互依赖性，尤其是国际层面上的这类问题，正潜在地影响相关主体理解和管理网络安全风险的能力。

1.2 IATA 大力拥护国际民航组织（ICAO）作为推动就航空网络安全开展协调一致的全球对话和行动的最合适组织。如果在航空网络安全方面没有明确的国际领导者，我们可能会面临全球标准支离破碎的风险，可能会看到复杂的监管体制阻碍增长和创新并限制我们评估和管理境内外航空网络安全风险的能力。

[1] 中文、阿拉伯文、英文、法文、俄文和西班牙文版本由国际航空运输协会提供。

1.3 虽然 ICAO“航空网络安全战略”有些迟来，但其制定仍是值得称赞的一步，IATA 对此全力支持。现在需要发挥领导力、拿出行动及适当的治理，通过修定现有大会 A39-19 号决议《解决民用航空的网络安全问题》以纳入相应参考资料，从而对该战略进行背书。因此，需要确保所有利益攸关方共同参与，确保适当的资源配置、时间和精力投入，也包括确保安全和安保。此外，继上述行动之后，重要的是鼓励各国批准《制止与国际民用航空有关的非法行为的公约》和《制止非法劫持航空器公约的补充议定书》。这种合作参与应能引发制定最佳做法和指导材料，对此 IATA 原则上支持制定与网络安全有关的标准和推荐做法（SARPs）及其后续执行和监督。

1.4 从更广的角度而言，在我们努力确保行业安全的过程中，我们不能忘记本行业的命脉，那就是我们的旅客和客户。我们必须确保在客户的整个旅程中，他们的网络安全、隐私、数据和权利都得到保护。此外，确保我们作为一个行业在这些问题上是透明的，这将确保我们与支持人士建立并维持信任关系。

1.5 IATA 一直积极致力于提高对全球航空网络安全挑战的认识和利益攸关方对话。IATA 有一个非常完备的航空器网络安全特别工作组（ACSTF），该工作组致力于增进了解，推动对话，并获取航空业利益相关方的最佳实践。ACSTF 已非常成熟，它创造了一个高度信任的环境，就大量相关主题分享和探讨了切实信息。此外，IATA 还邀请整个航空业的利益相关方在新加坡召开了一次具有突破性意义的航空网络安全圆桌会议（2019 年 4 月）。在这次圆桌会议上，利益攸关方探讨了航空业目前面临的挑战、网络安全的未来愿景以及如何实现这一愿景。调查结果突出表明，尽管目前已有很多工作正在进行中，但还有许多工作要做。

1.6 此外，IATA 已经启动了制定全行业的“航空网络安全战略”的流程，同时还包括起草实现该战略的路线图。该战略旨在让 IATA 能够代表其成员和整个行业，更多地关注我们面临的网络安全问题的挑战和机遇、关注切实的活动以带来改变，并关注为实现这一目标而开展的合作。

2. 讨论

2.1 基于当前增速，我们预计到 2037 年旅客数量将翻一番，其中大部分增长来自亚太地区[2]。这一增长将同时带来许多压力和风险，航空网络安全风险也是其中不可忽略的风险之一。必须确保增长所依赖的技术是安全、可靠、修复力强的，这一点非常重要，不可低估。

2.2 航空网络事件不仅仅会对安全、安保、运营服务、财务损失或增长产生影响。它可能会严重影响旅客对我们提供的服务的信心和信任。多年来，航空业已经证明了自己对安全或安保事件的适应能力，而且能够通过可见的措施和沟通来重建旅客信任。在发生不利的航空网络事件后，重建信任的难度将比航空业以往经历的困难更胜一筹，因此我们不仅需要改善网络安全，而且还需要就我们面临的挑战以及正在做出的努力进行公开对话。

[2] IATA 新闻稿（2018 年 10 月 24 日）。IATA 预测 2037 年航空旅客将达到 82 亿。可登陆网址 https://www.iata.org/pressroom/pr/Pages/2018-10-24-02.aspx阅览。

2.3 在我们推动技术进步的过程中，还必须在通过使用更多互联技术提高效率、改善服务与贯穿该技术整个生命周期的网络安全、安全和恢复能力之间找到平衡。除非某一技术在设计上本身就具有网络安全性，使用时同时运用主动、灵活的漏洞管理，以及供应商和最终用户之间建立透明的网络风险关系，否则航空业无法再接受任何新技术的引进。

2.4 在采取跨行业行动来改善网络安全的同时，还必须努力降低网络安全的成本。作为一个拥有各类组织的全球性行业，只要我们尽可能降低在良好应对网络安全风险方面的复杂性、成本或难度，那么任何国家（或公司）都不会掉队。

2.5 业界还应该采取更多行动，主动寻求网络安全风险和漏洞的可见性。这意味着对包括同行、国家、多国组织、其他行业和研究界在内的利益相关者之间的合作持开放、积极的态度。作为一个行业，我们必须非常清楚谁是我们的敌人，谁不是；那些希望帮助我们了解自身风险的人不是我们的敌人。跨部门、法律界和私人部门对硬件和软件网络漏洞的研究已经汇集成了一个繁荣而活跃的研究群体，他们真诚地帮助多个行业提高网络安全。

2.6 无论是通过何种方式得知，航空业有责任听取、评估任何潜在的安全问题，并酌情采取行动；当被告知潜在的网络安全漏洞时，我们也必须以同样的方式认真对待。航空业必须采取措施与研究界建立信任和关系，以便双方建立协作理解。IATA 也支持这一努力，并支持制定措施和立法以促进和保护善意研究人员支持航空业的能力。

2.7 2019 年 4 月在新加坡举行的 IATA 航空网络安全圆桌会议期间，来自整个行业的国际与会者强调了在哪些方面取得了进展，在哪些方面需要更多努力。要点如下。

2.7.1 对航空网络安全现状提出如下观点：

a) 事实证明，航空网络安全风险的规模和复杂性对一些组织构成了挑战，它们难以理解、难以确定优先次序或采取行动。

b) 由于航空业相互依存、覆盖全球，据评估，网络安全事件可能迅速扩大，并在全球造成影响。

c) 整个航空业在发现、管理和沟通网络安全漏洞方面仍然存在不一致和不足，导致实际网络安全风险的可见性较差。

2.7.2 与会者对 2030 年航空网络安全的理想‘未来愿景’以及如何实现这一目标提出了如下观点：

a) 网络安全文化。就像安全文化和实体安保文化一样，整个航空部门需要建立网络安全文化。

b) 透明度和信任。在所有航空业利益攸关方之间，需要在各种网络安全问题上 — 从获取网络安全相关数据到安全开发做法和漏洞管理等 — 增加透明度，从而增加信任。为了实现这一点，航空业可以运用它在安全和安保文化中已经采用类似做事方式，实现方法上的统一，并以一种大家都理解的方式产生共鸣。

c) 建立共识和一致性。在全球航空业，我们需要进一步建立网络安全一致性、标准和治理。这将需要组织和个人的领导力，以及所有利益攸关方进行公开对话的意愿。

d) 沟通和协作。为了更好地应对全球航空网络安全风险，必须在整个航空业内部以及航空业与能够提供帮助的外部门之间建立更牢固的关系。这将促进更紧密的全方位协作，无论是开发最佳实践还是管理潜在漏洞。

e) 劳动力。通过就航空业面临的网络安全挑战和机遇开展对话，我们必须激励能够支持应对航空网络安全挑战的新一代个人和组织。此外，必须教导航空人员如何识别和管理网络安全风险，从而提高警惕性和恢复力。

2.8 IATA 航空网络安全圆桌会议还讨论了另外两个议题。

2.8.1 调查事故或事件的网络安全方面。在航空事故和事件调查中，目前潜在网络安全问题的可见性很小。当众多航空系统已经实现连接和数字化时，迫切需要付出更多努力以了解如何捕获、有力保护和分析网络安全相关数据。不这样做的话，意味着该行业几乎没有能力自保或向客户保证其管理网络安全风险的能力。

2.8.2 总之，要提高航空业的网络安全、可靠和韧性，还有很多工作要做。但是，除了这一挑战之外，在所有利益相关方之间实现跨部门合作、采取行动并建立密切伙伴关系的潜力还很大。我们现在需要的是承诺、领导力和行动。

— 完 —