国际民用航空组织

工作文件

A42-WP/240
EX/102
29/7/25

大会 — 第42届会议

执行委员会

议程项目 13: 航空安保 – 政策

应急预案与网络演习作为提升应对网络威胁韧性的手段

(由巴西提交)

执行摘要

本工作文件强调需要根据对应国际民航组织航空网络安全战略支柱六的国际民航组织网络安全行动计划，为民用航空所用的关键系统建立应急预案，并根据对应战略支柱七的国际民航组织网络安全行动计划，同时结合基于此类系统实际特点和观察所得可导致网络攻击的事实进行模拟网络攻击训练演习的结果，改进此等预案。文件中还强调民用航空领域网络攻击的演变趋势，以及相关演习和应急预案的重要作用。

行动: 请大会鼓励各成员国:

a) 推动建立处理航空关键基础设施网络事件的管理计划; 和

b) 建立政府和私营部门利害攸关方都参加的定期网络演习制度。

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:	不适用。
查看文件:	国际民航组织航空网络安全战略支柱六 (事件管理和应急规划) 和支柱七 (能力建设、培训和网络安全文化)

1. 引言

1.1 网络威胁对民用航空业构成重大且日益严峻的挑战。作为一个本质上高度联通的全球体系，航空业中的漏洞可导致恶意软件迅速传播，产生广泛的全球性影响。尽管技术进步为航空业带来诸多益处，但对数字基础设施的深度依赖也催生了不断演变的网络威胁态势。国际民航组织《航空网络安全战略》认识到关键航空系统对网络安全和韧性的紧迫需要，基于七大支柱，概要阐述了各项相关原则、措施和行动。

1.2 因此，本工作文件谨概要介绍巴西在国际民航组织《航空网络安全战略》支柱六（事件管理和应急规划）和支柱七（能力建设、培训和网络安全文化）支持空中交通管制所用重要资产的网络保护的情况下，为提升网络韧性采取的若干措施。民用航空通过整合这两个支柱，可以构建一个全面且适应性强的防御体系，不仅能够应对威胁，还能主动预防和减轻其影响，确保航空旅行的持续安全性和可靠性。

1.3 支柱六包含强劲的复原程序，拥有清晰且经过检验的应急预案，能立即启动程序恢复受损系统和数据，确保将对空中交通管制、地面运行和乘客服务造成的干扰减至最小。其中包括备份、替代系统和详细的恢复步骤。

1.4 支柱 7 七则关注参与空中交通管制的各利害攸关方网络安全意识的提高和培训，确保从空管人员到地面维护人员人人掌握应对网络事件的方法，明了其在维护安全和安保环境中的作用。强大的网络安全文化意味着每个人都懂得自己可能会是第一道防线。同样，持续学习和适应也很重要，因为网络威胁形势是不断变化的，而且必须承诺适应新的网络安全策略和技术。这意味着绝不可安于现状，而是要不断努力进取。

1.5 这些原则对于加强民航网络安全机构与其他利害攸关方合作应对网络攻击至关重要，以造就一个稳固的应对态势，按应急预案从容应对恶意行为。文件应明确所有参与方之间的协调，详述每个系统遭受入侵后恢复正常运行可用的所有机制，强调对执行响应行动的关键要求，以促进构建一个更安全、韧性更强大的全球航空生态系统。

2. 讨论

2.1 每天媒体都会报道针对网络的攻击图谋，其中有些攻击得手了，而另一些则被公司和组织为应对此类日常攻击实施的各种防护措施所阻止而未见报道。航空领域的现实情况也并无二致。攻击者主要寻找未补的漏洞，试图入侵系统，窃取信息并修改系统，通常都是为了取得经济利益。

2.2 巴西通过巴西空管局（DECEA）一直在采取措施，以增强巴西空中管制系统在日益严峻的网络威胁背景下的韧性。因此，DECEA 的举措与国际民航组织对此一问题的理解相一致，并体现了国际民航组织网络安全战略中提到的两大支柱。DECEA 还一直推动演习，以培训空管机构的应急响应团队。除促进团队培训外，这些演习还有助于识别为满足空中交通管制的运行需要开发的系统和应用程序的组合导致产生的网络安全漏洞。此等培训演练的结果被写成报告，提交给负责改进系统和应急预案的团队。

2.3 关于演练，每种模拟情景均附有相关系统维护专家提供的详细信息，以确保情景的现实可靠性。因此，演练行动更贴近实际情景，更能准确进行评估，并结合对每一系统（查明的差距）以及计划本身所采取的行动，提出针对性改进意见。

2.4 国际民航组织网络安全战略的另一个支柱是事件管理和应急规划，为巴西空中管制所用的每一关键系统制定相应的应急预案提供了基础。该文件详细描述了为恢复各系统在空管不同层级的功能而采取行动所需的全部必要信息，以及参与响应的各方适当协调，以最大限度地减少停机时间，降低对航空运输用户的影响。

2.5 应急预案是根据 ISO/IEC 27031 等国际标准制定的，并按照每个地点的具体情况进行调整。因而得以总成每个地点系统功能的详细信息，即使在遭受网络攻击时也能维持这些功能，保持整个环境的韧性和可控度。

2.6 必须说明的是，巴西空管局还参加了由国防部负责的巴西国家网络安全演习，其目的在于保护国家的关键系统。在此一全国性演习中，DECEA 向航空运输安保方面贡献了其空管单位积累的专业经验，也了解了同样拥有关键系统且需保护和韧性措施的其他领域的情况。这次全国大演练中开展的活动，有助于验证和完善应急预案，而应急预案面对每日新的威胁是需要不断更新的。

2.7 巴西呼吁国际民航组织成员国及航空业界支持并组织网络安全演习，集合政府与行业专家，共享在培训网络专家应对网络攻击和制定更可靠网络应急预案方面的最佳实践和专业经验，以保护航空关键基础设施和系统。

3. 结论

3.1 网络威胁是一个无所不在的挑战，而民用航空业以其精密复杂的全球网络具有同样的脆弱性。巴西采取的主动出击立场，如 DECEA 各项举措所展示的，与国际民航组织的航空网络安全战略高度契合，尤其是该战略的支柱六和支柱七。强调按照 ISO/IEC 27031 等国际标准并结合本地具体情况制定有力的应急预案，同时开展定期、现实的网络演习，可显著提升网络的韧性。这些努力不仅能培训事件响应团队，查明漏洞所在，还能在所有利害攸关方中建立强大的网络安全文化。通过分享专业经验和参加国家和国际演习，巴西强调了为保护全球航空生态系统免受不断变化的网络风险侵袭，而不断适应并采取集体行动的急迫需要。

— 完 —