国 际 民 用 航 空 组 织

工 作 文 件

LC/39-WP/2-5[1]
10/5/24

法律委员会 — 第 39 届会议

（2024 年 6 月 25 日至 28 日，蒙特利尔）

议程项目 2：审议法律委员会总体工作方案

引起国际民用航空界关切但现有航空法文书规定可能未予充分涵盖的行为或侵犯行为，包括网络威胁

（由多米尼加共和国提交）

1. 背景

1.1 国际民航组织大会第 41 届会议确定，引起国际民用航空界关切的某些行为或犯罪，包括网络威胁，可能未在现有航空法文书中充分涵盖；因此，应对这些威胁的做法一直侧重于网络安全方面的法律工作。我们的理解是，近几十年来在这方面所做努力始终是为了适应当前的问题。2022 年，秘书处向在蒙特利尔举行的法律委员会第 38 届会议提交了一份法律问题研究分组的报告，其中指出，现有的国际航空法框架只部分足以充分应对针对民用航空的网络威胁。

1.2 随后，在民航法律顾问论坛（2019 年 5 月 16 日和 17 日）议事记录中，新加坡提交了研究结果并提出建议，大意是“网络安全带来的挑战和脆弱性是数字时代的副产品。这一问题不仅存在于航空活动中，也涉及我们社会的所有活动。因此，从法律角度来看，航空业的问题也可以像其他部门一样得到处理”。应不遗余力地应对民用航空安保所面临的网络挑战，重点采取全面行动，以便在所有部门相关领域都采取措施。否则，将会出现更多的法律空白。

1.3 我们同意 2019 年国际民航组织《航空网络安全战略》中所述内容：“关于民用航空网络安全的国际、地区和国家立法与规章的主要目的是支持实施全面的网络安全战略，以保护民用航空和旅行公众免受网络攻击的影响。”《战略》进一步指出，各国“必须确保在实施国家民用航空网络安全政策之前，按照国际民航组织的规定制定和采用适当的立法和规章。”显然，在技术方面已经取得了显著进展，航空方面的发展也因此卓有成效。因此，各国都采取了与数字化转型、网络攻击、网络威胁、隐私和数据保护有关的措施；这也意味着，在某些情况下，可能没有必要修订涉及纳入网络安全相关方面的国家和国际指导、指南、政策和条例，特别是运行和航空安保方面。

1.4 根据国际民航组织 2022 年《网络安全行动计划》，“鼓励各国评估其网络安全和民航领域的国家现行法律框架，以确定现有的差距，并确保针对具体的民航网络安全内容落实适当的立法和规章。另一个关键要素就是鼓励其国家法律框架中仍没有执法机制的国家建立执法机制，以便对使用网络手段针对民用航空的非法行为进行刑事定罪和追诉。”

---

[1] 西班牙语版本由多米尼加共和国提供。

2. 分析

2.1 2019 年，根据民航组织《航空网络安全战略》的指示，各国须考虑各自国家立法是否需要更新或者通过新的国家立法，以允许起诉有关恐怖主义的网络攻击以及对民用航空产生不利影响的攻击。毫无疑问，相关法律法规现已存在。然而，鉴于在法律上，如正确实施相关制裁，罪行的界定至关重要，因此各国迫切需要制定明确和统一的指南。仅仅认识到网络安全在国际民用航空中的重要性是不够的。相关指南已经发布，但技术的发展比我们的更新速度更快，我们仍需努力赶上当前的发展。现在正是确定各国在这一领域的法律义务和责任的时机。

2.2 虽然存在自愿性的非约束性标准和非自愿性的约束性标准，如附件 17 中规定的标准；仍有必要确定如何在这方面适用国际法原则，同时更全面地制定国家规范。目前各国在立法或技术方面仍存在局限性，因此我们无法忽视被认为已得到补救的情况受到威胁的可能性。

2.3 在多米尼加共和国，第 53-07 号法（2007 年）等立法涵盖了高科技犯罪和违法行为。不过，我们认为，该法或多米尼加共和国的《刑法典》不一定涵盖或能够界定已经出现或今后可能出现的对民用航空的网络威胁。此处所指为网络恐怖主义和网络间谍，以及对关键基础设施的攻击。此外，检察院受理的大多数案件都涉及对私人申诉的公开执行，即受影响者必须提出申诉，并在整个诉讼过程中与检察院合作，这可能意味着被告逍遥法外。在法律界定时，必须确保受理的任何案件都是纯粹的公共案件。

2.4 监管机构倾向于对信息和通信技术（ICT）或运行技术中的威胁和/或缺陷进行分类。毫无疑问，近几十年来，在所有行政和技术事务中，信息和通信技术的安全问题明显受到重视。然而，运行技术的情况并非如此，因为在空中航行和飞行规则等领域，某些保障措施的实施是以其运行效率为代价的；有效性还是安全性始终是争论不休的问题。

2.5 多米尼加共和国根据《宪法》，特别是《宪法》第 260 条采取措施，确保技术发展及其对民用航空的影响不会危及安全，并指出“国家的优先目标是：打击危及国家及其居民利益的跨国犯罪活动；组织和维持制度的有效性，以防止或减轻自然灾害和技术灾害造成的损失”。

2.6 随后，根据 2018 年 6 月 19 日发布的第 230-18 号法令制定了《2018-2021 年国家网络安全战略》，并成立了国家网络安全中心。网络事件响应小组（CSIRT-RD）作为全国性的联络点，负责预防、检测和管理影响政府信息系统和关键基础设施的网络事件。

2.7 2024 年，多米尼加共和国国会正在审议一项关于多米尼加共和国网络安全综合管理的法案，该法案旨在加强全国公共行政信息和通信技术基础设施和关键基础设施的网络安全管理的监管框架。一旦该法案获得批准，多米尼加共和国将成立国家网络安全委员会，作为国家网络安全中心的合议机构和最高权力机构，负责制定和指导与公共行政信息和通信技术基础设施和关键基础设施有关的网络问题管理政策。

2.8 该法案认可 2018 年 11 月 12 日《网络空间信任与安全巴黎倡议》和 2019 年 11 月全球网络空间稳定委员会最终报告中提出的原则。它不加区分地涵盖了互助、防止非法活动、信息交流、保护人权和保护关键基础设施等原则。

2.9 必须说明的是，尽管国家网络安全中心自 2018 年以来就已存在，但根据该法案，它将作为一个隶属于总统府、具有法人资格以及职能、预算、行政、技术和财政自主权的公法实体；其宗旨是使国家网络安全中心在履行职能时拥有更大的独立性。

2.10 同样，该法案还讨论了关键基础设施和网络安全事件信息，即如何识别网络安全事件、指定网络安全事件所依据的框架、相应的行政程序和风险分析。该法案还界定了重大网络影响和处罚制度。该法案力争涵盖迄今为止尚未考虑的问题。

3. 结论

3.1 显然，在面对网络安全威胁和网络安全事件时，若要成功采取行动，必须制定框架以规范采取各项预防措施、管理有效应对措施以及监管相关基础设施。我们面临的形势影响每一个人和每一件事，因此，我们必须予以正视。多米尼加共和国将网络安全视为国家安全问题，因此相应地采取了措施。

3.2 我们鼓励尚未采取此类行动的其他国家以同样的热情采取行动。我们建议所有尚未考虑这一问题的国家评估其刑法、刑事和程序立法情况，将这类犯罪视为危害国家安全的公共行为。我们还敦促在法律中更新并纳入网络恐怖主义和网络间谍等刑事犯罪，以便对其提起诉讼和进行适当界定，从而在国家和国际层面保护航空安保。此外还应扩大术语范围，将过去十年中出现的新型网络攻击和网络威胁包含进来。

— 完 —