【航空法研究】

欧盟民航网络安全立法的发展与启示

——以欧盟《网络与信息系统安全指令 2.0 版》为例

解晓丹

（华东政法大学 国际法学院，上海 200042）

摘　要：为应对网络威胁，建立一体化的欧盟网络安全体系，欧盟于 2016 年颁布了《欧盟 2016/1148 号指令》。然而，由于欧盟各成员国的实践存在差异和冲突，该指令没有达到理想的实施效果。为了消除分歧并适应网络威胁的新变化，欧盟于 2022 年 12 月颁布了《网络与信息系统安全指令 2.0 版》，将三类民用航空实体纳入“基本实体”的管辖范畴，并规定了网络安全风险管理措施以及网络威胁事件报告等义务。《中华人民共和国网络安全法》为我国网络安全工作提供了战略指导和法律依据，但在民航领域欠缺具体细则。我国可借鉴欧盟《网络与信息系统安全指令 2.0 版》，通过构建完善的民航网络安全术语体系、规范民航网络安全义务主体、细化民航网络安全管理措施、完善网络安全事件报告义务等措施来推动民用航空网络安全立法的发展与完善。

关键词：民用航空；网络安全；《网络与信息系统安全指令 2.0 版》；网络安全法；网络与信息系统

中图分类号：D 922.16　　**文献标识码**：A　　DOI：10.13486/j.issn.2097-4973.2025.01.007

近年来，随着航空运输需求的持续增长，民用航空业经历了数字化转型。然而，对网络信息技术的高度依赖，导致民航业面临严峻的网络安全威胁风险。2015 年 4 月，美国联邦航空管理局的行政计算机系统被黑客以电子邮件的方式植入病毒。[1] 同年 6 月，波兰航空公司（LOT Polish Airlines）的计算机系统遭到黑客攻击，导致该计算机系统无法向航空器发送说明飞行路线、天气和其他重要信息的飞行计划，造成 10 个航班停飞、约 15 个航班延误，大约 1 400 名旅客的出行受到影响。[2] 2017 年 6 月，乌克兰最大的航站楼鲍里斯皮尔国际机场（Boryspil International Airport）遭到网络攻击，该机场的计算机和旅客登机牌系统因此瘫痪。[3] 民航网络受到攻击的类型、频率、规模和复杂程度正在不断增加，对民航网络安全提出了更高的防护要求。

为了应对日益严峻的网络安全威胁，提高欧盟抵御网络安全威胁的能力，欧盟于 2016 年颁布了《欧盟 2016/1148 号指令》，即第一代《网络与信息系统安全指令》（NIS Directive）。欧盟各成员国按要求相继实施网络安全监管措施，推动了欧盟网络安全防御能力的建设和发展。由于各成员国在关于网络安全的要求类型、详尽程度、监督方法等方面存在差异，甚至出现了一成

收稿日期：2024-10-06

基金项目：华东政法大学研究生创新能力培养专项计划项目“民航涉外法治建设视角下的航空旅客保护立法完善研究”（2024-3-022）

作者简介：解晓丹（2000—　），女，广东肇庆人，在读硕士研究生，主要从事国际法研究。

E-mail：xiexiaodan2022@163.com

员国与另一成员国的要求相冲突的情况，导致该指令的实施效果大打折扣。与此同时，网络安全事件的数量、规模、频率和影响不断扩大，对网络与信息系统的运作构成重大威胁。2021 年 7 月，欧盟网络安全局（ENISA）预测 2021 年的供应链攻击数量可能是 2020 年的 4 倍①，但第一代《网络与信息系统安全指令》并未涉及供应链安全的具体问题。为此，2022 年 12 月，欧盟废除了《欧盟 2016/1148 号指令》，颁布了《欧盟 2022/2555 号指令》，即《网络与信息系统安全指令 2.0 版》（NIS 2 Directive，以下称“《指令 2.0》”）。《指令 2.0》进一步细化了网络安全管理措施和事件报告等义务，为各成员国转化立法提供了更加明确的要求和指引，从长远来看，有助于推动建设欧盟一体化的网络安全。

习近平总书记在 2018 年 4 月 20 日召开的全国网络安全和信息化工作会议上强调，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。[4] 民航业作为一个高度依赖网络和信息化的行业，与人民群众的利益息息相关，重视民航网络安全建设是贯彻总体国家安全观、落实人民至上理念的体现。《指令 2.0》代表了欧盟网络与信息系统安全建设立法的最新进展，在明晰管辖主体、网络安全义务等方面呈现出创新性发展，对我国加强网络安全合作、统筹民航网络安全建设具有一定的借鉴意义。本文旨在以欧盟网络与信息系统安全法律治理框架研究为基础，分析我国民航网络安全立法的现状与不足，并为我国搭建民航网络安全治理框架提出相应的建议。

一、欧盟《指令 2.0》的主要内容

（一）《指令 2.0》的主要变化

《指令 2.0》扩大了管辖主体的范围。《指令 2.0》以部门（sector）的数字化、互联程度以及对经济和社会的重要性为标准，将管辖的部门从 19 个增加到了 35 个，除了原有的能源、交通、银行业、金融基础设施等部门，邮政服务、废弃物管理、食品、化学品生产和分销以及农产品等不属于《欧盟 2016/1148 号指令》管辖的部门也被纳入其中。《指令 2.0》同时列举了部门所涵盖的具体实体（entity），也即根据其设立地国家法律设立并被承认、以自己的名义行使权利并承担义务的自然人或法人。以航空部门为例，《指令 2.0》列举了航空承运人、机场和机场管理机构三类实体。《指令 2.0》还为成员国留下了一定的酌处权，成员国有权识别那些规模不大、但具有高安全风险的实体，并将其涵盖在《指令 2.0》的管辖范围内。

《指令 2.0》取消了“基本服务运营商”（operators of essential services）和“数字服务提供商”（digital service providers）的实体划分。《欧盟 2016/1148 号指令》将管辖的实体划分为“基本服务运营商”和“数字服务提供商”，但是这样的分类方式并没有反映实体对经济社会的重要性，违背了依据实体的经济重要性程度来设定不同义务的初衷。《指令 2.0》不再区分这两类实体，而是引入了新的实体划分方式，根据部门的关键程度和规模将实体划分为“基本实体”（essential entities）和“重要实体”（important entities），并设置了不同的监管制度。相较于重要实体，基本实体对网络服务产生更大的影响，须遵守更严格的监督义务。这种概念划分在表达上更为简洁，且反映了实体与经济社会的联系程度，有助于成员国更好地理解和确定本国的相关义务实体，确保更统一地履行义务。

除此之外，《指令 2.0》还简化了所涵盖实体在遭受网络安全威胁事件之后进行事件报告的义务，以免过度报告给义务主体带来过重的负担。《指令 2.0》还更新了部分条款，与包括金融部门法案在内的具体部门立法保持一致。

（二）《指令 2.0》规定在民航领域的义务主体

《指令 2.0》附件一通过列举的方式将三类民航实体纳入了“基本实体”的范畴。第一类是根据《欧盟 300/2008 号条例》第 3.4 条定义的用于商业目的的航空承运人，即持有有效运营许可证或同等资格的航空运输企业。第二类是根据

① 参见欧盟网络安全局（ENISA）2021 年 7 月发布的《供应链攻击威胁图谱》。https://data.europa.eu/doi/10.2824/168593.

《欧盟2009/12/EC号指令》第2条第1点定义的机场,以及第2条第2点规定的机场管理机构。第三类则是《欧盟549/2004号条例》第2条第1点定义的提供空中交通管理服务的运营商。作为《指令2.0》定义的基本实体,上述三类民航实体需要履行相关义务。

(三)《指令2.0》下民航主体的核心义务

第一,实施网络安全风险管理措施的义务。《指令2.0》第21条要求上述三类民航实体实施网络安全风险管理措施(cybersecurity risk-management measures),采取适当和相称的技术、成立必要的机构来组织和管理网络安全风险,这些措施旨在保护民航网络和信息系统以及系统所处的物理环境免遭事件影响,并最大限度地减轻事件对用户的影响。在《指令2.0》第6条,"风险"(risk)、"事件"(incident)与"网络和信息系统安全"(security of network and information system)等术语得到了明确定义。《指令2.0》将"风险"一词定义为"事件造成损失或干扰的可能性",在判断这一可能性时应综合考虑损失或干扰的规模与事件发生的概率。"事件"又被定义为"对存储、传输或处理的数据或网络和信息系统提供的或通过网络和信息系统获取的服务的可用性、真实性、完整性或保密性造成损害的事件"。"网络和信息系统安全"指的是"网络和信息系统在一定的可信度下抵御任何可能危及所存储、传输或处理数据的可用性、真实性、完整性或保密性,或危及由这些网络和信息系统提供的服务或通过这些网络和信息系统获取的服务的能力"。

综合上述定义,网络安全风险管理措施在民用航空法的语境下可以理解为:欧盟各成员国的民航安全实体必须管理事件造成损失或干扰的可能性,使民航安全实体用于其业务或提供服务的网络和信息系统能够在给定的可信度下抵御任何事件。具体来说,《指令2.0》第21条规定的网络安全风险管理措施包括以下内容:风险分析和信息系统安全政策;事件处理;业务连续性,如备份管理和灾后恢复,以及危机管理;供应链安全,包括涉及每个实体与其直接供应商或服务提供商之间关系的安全;网络和信息系统购置、开发和维护的安全,包括漏洞处理和披露;评估网络安全风险管理措施有效性的政策和程序;基本网络卫生做法和网络安全培训;有关使用加密技术和在适当情况下使用加密技术的政策和程序;人力资源安全、访问控制政策和资产管理;在实体内酌情使用多因素认证或持续认证解决方案、安全语音、视频和文本通信以及安全应急通信系统。通过上述十类措施,欧盟建立起了一套事前预防、事中响应、事后恢复的网络安全威胁应对制度。

在网络安全威胁的事前预防方面,《指令2.0》下的民航实体需要制定风险分析和信息系统安全政策,评估网络攻击对其最重要资产的潜在影响,并对潜在的网络漏洞保持警惕。在风险分析和系统安全政策制定完成后,民航实体还须对该政策的有效性展开评估。民航实体有义务关注网络与信息系统的获取、开发和维护方面的安全,并及时披露和处理漏洞。为了提高工作人员应对网络安全威胁的素质和水平,《指令2.0》要求民航实体加强对相关工作人员的网络安全培训。《指令2.0》还强调供应链安全,包括每个民航实体与其供应商或服务提供商之间的安全关系维护。在网络威胁事中响应和事后恢复方面,《指令2.0》规定的义务较为简单。各民航实体有义务实施事件处理措施,包括在网络威胁事件发生后第一时间进行响应的系统步骤和对威胁事件保持持续检测。《指令2.0》强调了各实体的业务连续性,要求民航实体在遭受网络攻击的情况下仍然有能力保持运营,这就意味着民航实体要制定一套灾后恢复以及最大限度地减少干扰的方案。

第二,事件报告义务。根据《指令2.0》第23条第1款,上述三类民航实体必须向当局报告任何对其提供的服务产生重大影响的网络安全事件。在欧盟立法中,事件报告义务屡见不鲜。例如,在电子通信网络和服务部门,报告安全漏洞的义务已存在十多年。此外,欧盟2016年《通用数据保护条例》(General Data Protection Regulation,简称"GDPR")第33条也规定了在严格时间范围内向监管机构通报个人数据泄露事件的严格义务。为了提升网络与信息系统的网络安全弹性,《欧盟2016/1148号指令》引入了类似的事件报告义务,其中第14条要求成员国

确保基本服务运营商在发生对其服务连续性产生重大影响的事件时，及时通知主管当局。在确定“重大影响”的程度时，由于各成员国的评估标准不同，同一个安全事件在一国属于报告的范围，而在另一国并不需要报告，不同国家当局收到报告的数量差异很大。例如，2018 年，匈牙利当局收到了 900 份事件报告，而立陶宛当局收到了 10 000 份报告。[5] 为了避免各成员国实践差异过大带来的实施碎片化问题，《指令 2.0》在保留对事件报告义务的基础上，对义务主体做出了更加精确细致的规定。

《指令 2.0》明确了“重大影响”事件的范围。在评估“重大影响”的程度方面，《欧盟 2016/1148 号指令》仅列举了受影响的用户数量、影响时间和地理范围这三个因素供成员国参考，在实践中各成员国评估结果差异很大。《指令 2.0》摒弃了这种评估方法，在第 23 条第 3 款直接规定了两种重大事件的情况：一是该事件已经造成或能够造成有关实体服务的运作中断或财务损失；二是该事件已经影响或能够影响其他自然人或法人，造成严重的物质或非物质损失。只要某一事件满足其中之一，就属于需要报告的重大影响事件。

《指令 2.0》对事件报告的程序、通知内容和必须报告事件的时限做出了更加精确的规定。根据《指令 2.0》第 23 条第 4 款，在该重大事件发生后，各民航义务主体需要在首次意识到事件发生后的 24 小时内发出“预警”(early warning)，说明有关事件的一些基本信息。例如，事件是否被怀疑是非法或恶意造成的，以及它是否有可能产生跨境影响等。在首次意识到事件发生后的 72 小时内，各民航义务主体应更新报告，提供更全面的“事件通知”(incident notification)，除了“预警”中的内容外，还应包括对事件严重性、影响和折中指标的初步评估。在“事件通知”后的一个月内，民航义务主体应提交一份详细的“最终报告”(final report)，对该事件进行详细描述，说明可能引发该事件的威胁和根本原因，已经采取了和正在采取哪些缓解措施，以及事件是否最终造成跨境影响等等。

(四)民航实体违反义务的后果

《指令 2.0》为欧盟各成员国设立了一个一致的处罚框架，并对基本实体和重要实体的监督制度进行了区分，以确保二者的义务得到平衡。在行政罚款方面，《指令 2.0》第 34 条为基本实体违反网络安全风险管理义务和事件报告义务的行为制定了一个最高限度的行政罚款标准。如果上述三类民航实体违反了网络安全风险管理义务和事件报告义务，将会受到 1 000 万欧元以下或者最高不超过企业上一财政年度全球营业额总额的 2% 的行政罚款。成员国须在自己的国内法中对行政罚款做出细化规定，确保罚款的相关规定有效、适度和具备劝阻性。

二、欧盟《指令 2.0》对完善我国民航网络安全立法的启示

(一)我国民航网络安全立法的现状

目前，我国有关于民航网络安全的主要法律和行业标准包括：2016 年颁布的《中华人民共和国网络安全法》(以下简称《网络安全法》)、中国民用航空局(以下简称民航局)于 2018 年发布的行业标准《民用航空网络安全等级保护定级指南》(以下简称《定级指南》)与 2020 年发布的行业标准《民用航空网络安全等级保护基本要求》(以下简称《基本要求》)。此外，交通运输部曾于 2017 年 2 月 20 日公开征求《民航网络信息安全管理规定(暂行)》的意见，但该规章至今仍未正式颁布。

第一，《网络安全法》的规定。《网络安全法》是我国网络安全领域的基础性法律，虽然其并未专门针对民航网络安全保护进行细化规定，但其项下的关键信息基础设施保护制度与民用航空网络安全紧密相关，因此《网络安全法》的相关规定也同样适用于民航信息系统的网络安全保护。《网络安全法》第 3 章第 2 节以相当的篇幅规定了关键信息基础设施保护制度，涵盖了公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域。[6] 作为交通领域的重要部门之一，民航部门亦在《网络安全法》的管辖范围之内。根据《网络安全法》第 34 条的规定，民航部门需要履行四项主要的安全保护义务：一是设置专门安全管理机构和安全管理负责人；二是定期对从业人员进行网络安全教育、技术培训和技能考核；三是对重要系统和数据库进

行容灾备份；四是制定网络安全事件应急预案，并定期进行应急演练。

第二，民航局发布的行业标准。除了法律法规之外，民航局发布了多项关于民航网络安全的行业标准，以指导民航网络安全保护工作。虽然这些行业标准不属于严格意义上的法律渊源，但在实践中发挥了重要的指导作用。其中，《定级指南》规定了民航业网络安全等级保护的定级原理、方法和等级变更等相关内容。根据《定级指南》，民用航空网络安全保护等级共分为五个等级，定级的依据主要依赖于两个“一级要素”：一是等级保护对象受到破坏时“所侵害的客体”，二是“对客体造成侵害的程度”。

根据民用航空网络与信息系统的业务信息和系统服务特征，《定级指南》将一级要素“对客体的侵害程度”进一步分解为两个二级要素，即“业务重要性”与“网络与信息系统规模”。其中，业务重要性指的是网络与信息系统承载业务的重要程度，可分为一般、重要、核心三个级别。业务越重要，对客体的侵害程度就越严重。而网络与信息系统规模则可以通过运输业务量和服务的地理范围这两个指标进行评估。业务量越大、地理范围越广，则对客体的侵害程度越严重。定级流程分为五个步骤，包括确定定级对象、初步确定等级、专家评审、主管部门审核、公安机关备案审查。

在定级工作完成后，《基本要求》对不同等级的保护要求进行了逐步细化，规定了民用航空网络安全等级保护的第一级到第四级等级保护对象的安全通用要求和安全扩展要求。这些要求主要涉及民航网络安全保护对象的物理环境、通信网络、安全运营管理和安全事件处置等方面。至于第五级的等级保护对象，由于其涉及对国家安全的特别严重损害，因此被视为极为重要的监督管理对象。这类对象具有特殊的管理模式和安全要求，因此不在《基本要求》规定范围之内。

（二）我国民航网络安全立法的局限

以《网络安全法》作为依托，并配合民航局发布的相关行业标准，我国民航网络安全法律制度得以初步建立。然而，我国现行民航网络安全法律体系仍存在一定的局限性，亟须在总结其现有问题的基础上，参考欧盟《指令 2.0》的相关规定，完善民用航空网络安全法律制度。

我国民航网络安全领域存在立法空白。《中华人民共和国民用航空法》是我国现行的唯一一部民用航空法律，涵盖了民用航空器的国籍、权利、适航管理、航空人员等传统领域的内容，但未涉及民用航空网络安全等新兴问题，缺乏对民用航空网络安全的有效规制。在现有法律体系中，尽管有《中华人民共和国民用航空安全保卫条例》、《中国民用航空应急管理规定》等行政法规和部门规章，但它们的关注点多集中于有形的非法干扰行为和突发事件，例如随意穿越航空器跑道、滑行道等行为，对民用航空网络安全相关内容的规定显得相对薄弱。民航局颁布的《定级指南》和《基本要求》虽然是专门针对网络安全的规范性文件，但只针对事件发生之后对其进行定级评估相关的内容，难以涵盖民用航空网络安全保护的全过程。民用航空网络安全需要环环相扣、结合紧密的保护措施，不仅要在事件发生之后进行评估，将事件损失降到最低，更要关注和完善事件发生前的基础防御、紧急预案等。

《网络安全法》中关于网络安全相关术语的界定不够清晰具体，网络安全保护义务也呈现出概括性、原则性的特点，缺乏对民航行业的专项规定。欧盟《指令 2.0》对包括“网络与信息系统”、“网络安全”、“事件”、“事件处理”、“云计算机服务”、“信用服务”和“数字服务”等在内的41个与网络安全有关的术语做出了定义。相比之下，《网络安全法》第76条的术语定义中只包含“网络”、“网络安全”、“网络运营者”、“网络数据”和“个人信息”这五个概念，未能涵盖更多与网络安全密切相关的术语。此外，《网络安全法》所规定的义务具有高度概括性和通用性，需要出台民航领域具体的专项法律以明确相关主体更细致具体的法律义务。

（三）完善我国民航网络安全立法的建议

在总体国家安全观的指引下，《网络安全法》为我国的网络安全工作提供了战略指导和法律依据。然而，作为我国网络安全保护的顶层设计，《网络安全法》本身具有高度概括性和通用性，并不是针对民航领域的法律。鉴于民航业面临的特殊安全挑战和技术环境，可以在参考欧盟《指令 2.0》中的网络安全管理措施义务及事件

报告义务等核心内容的基础上，以《网络安全法》为依托，由民航局牵头，结合民航规章制定专家组意见，制定一部专门的《民航网络信息安全管理规章》，根据民航业的特点针对民航领域的特殊情况做出细化规定。[7] 具体来说，我国民航网络安全立法应包括以下内容。

第一，构建清晰完善的民航网络安全术语体系。清晰的法律定义有利于明确法律的指向，提供法律思维框架，是实现法治的重要前提。[8] 与欧盟《指令 2.0》中全面且细致的网络安全术语相比，我国《网络安全法》在网络术语的定义上存在数量较少、内容较为概括的问题。除了法律层面的规定外，民航局发布的行业标准也仅对“网络安全”、“安全保护能力”、“关键信息基础设施”等少数术语进行了简要说明，未能完全有效发挥指导作用。网络安全本就是十分复杂和专业的领域，更需要对各种网络安全术语进行清晰地定义，以确保为《网络安全法》和民航局行业标准的正确理解与适用提供有效支撑。因此，可以参考欧盟《指令 2.0》，对我国民航网络安全所涉及的专业术语进行一次梳理。

在民航自身网络安全能力方面，除了需要对“网络”和“网络安全”做出更清晰的解释外，还需要增加“网络与信息系统”、“信息通信技术”、“技术规范”、“域名”、“电子通信”等与民航运营安全有关的术语定义。在保护旅客信息方面，需要在《网络安全法》的“个人信息”定义的基础上，根据旅客信息的收集、使用和保护等环节，进一步明确“旅客信息”、“旅客信息安全”等术语的定义。通过建立一套清晰完善的民航网络安全术语体系，为民用航空领域的网络安全管理提供更加明确的操作标准，进一步促进民航网络安全保护工作的开展。

第二，确定“网络运营者”在民航领域的具体实体。根据《网络安全法》第 76 条的规定，网络运营者是指网络的所有者、管理者和网络服务提供者，然而该定义未对具体实体做出列举。与之相较，欧盟《指令 2.0》根据部门的关键程度和规模，将实体划分为“基本实体”和“重要实体”，并对两类实体设定了不同的义务。《指令 2.0》明确将三类民航实体划分至“基本实体”的范畴，对这三类民航实体的义务做出了严格规定。

民航活动的有序运行离不开网络技术的支持，机票预订、旅客安检、行李托运、空中交通管理信息以及航空器的平稳运行等都依赖于网络信息系统。鉴于这些核心功能的网络化特征，在我国民航网络安全立法的框架下，需要明确哪些民航实体应当被认定为“网络运营者”。按照《网络安全法》中对“网络运营者”定义的逻辑，民航领域的“网络运营者”至少应当包括机场服务运营者、承运人、空中交通服务提供者及其他民航相关网络服务供应商等实体。通过对民航领域的“网络运营者”进行界定，有助于明确各类民航主体在网络安全管理中的责任与义务。

第三，依托《网络安全法》细化民用航空网络安全管理措施。一套完整的民航网络安全管理体制是提高民航网络安全能力、有效防范民航网络威胁的关键。欧盟《指令 2.0》要求民航相关实体承担网络安全风险管理和事件报告义务，提高了欧盟应对网络安全威胁的能力。我国民航网络安全立法可以借鉴欧盟《指令 2.0》的做法，将《网络安全法》下民航实体的网络安全义务具体落实到民航网络安全实践措施方面。

首先，可以根据《网络安全法》第 34 条的规定，在民航领域对相关义务进行细化。例如，设置民航网络与信息安全事件响应小组、民航局信息安全主管部门、民航安全监督管理局等专门安全管理机构，协调各主管部门的职责，在国家层面开展民用航空网络安全合作。[2] 其次，定期对民航从业人员进行网络安全教育、技术培训和技能考核，提高从业人员应对民航网络安全威胁的素质和应急处理能力。这不仅有助于提高民航从业人员的安全意识，还能增强整体应对网络威胁的能力。最后，建立网络威胁情报共享机制。当民航实体在受到网络安全威胁时，应在规定的时间内向民航网络安全管理机构提交报告，并通过搭建民航网络威胁信息共享情报网，增加民用航空网络安全威胁情报的透明度，以提高预防威胁的效果和能力。

第四，结合民航网络安全等级保护制度完善事件报告义务。民航局发布的《定级指南》和《基本要求》对民用航空网络安全保护进行等级划分，共设五个等级，并根据各等级的重要程度，规定了相应的安全保护义务。欧盟《指令 2.0》为

民航主体设定了事件报告义务，民航实体必须向当局报告任何对其服务的提供产生重大影响的网络安全事件，并对“重大影响”做出了定义。因此，可以在保留我国民航网络安全保护现有的定级制度的基础上，参考欧盟《指令 2.0》，进一步完善我国民用航空网络安全事件报告义务。在现有的民航网络安全等级保护体系基础上，进一步完善定级制度，更新定级的标准和细则，加强对民航网络安全的日常检查和监督工作，确保民航系统网络安全能力符合各级保护要求。借鉴《指令 2.0》的经验，细化民航领域的事件报告义务。根据民航网络安全保护等级的不同，网络安全事件可以按其对运营服务的影响程度进行分类，并要求民航实体根据事件的重要性提交不同层级的报告。具体来说，较为严重的安全事件应在短时间内报告，并在事后提供详细的事件信息；而影响较小的事件则可在较长时间内报告，报告内容可相对简洁。这种分级报告制度有助于提高事件处理的效率，并确保相关方面能够及时获取关键信息，进行有效的应对与决策。

三、结论

《指令 2.0》是欧盟在对《欧盟 2016/1148 号指令》六年实施经验进行总结的基础上，在网络与信息系统保护方面的最新立法成果。《指令 2.0》规定的事前预防、事中响应和事后恢复的网络安全威胁应对机制，以及网络威胁事件报告义务等都得到了创新性的发展和巩固，值得我国在制定民航网络安全法律时进行参考。

2022 年，我国民用航空局、国家发改委、交通运输部联合印发的《“十四五”民用航空发展规划》明确指出，网络安全是民航安全管理的重要组成部分，也是智慧民航体系建设的根基与保障，要健全网络安全管理制度，提升技术防护与应急处置能力，强化关键信息基础设施和重要数据资源的综合保障，确保行业安全稳定运行。面对网络攻击手段日益多样化、复杂化和隐蔽化的趋势，我国民航亟须在法律制度层面推进网络安全体系的统一与完善。当前，《中华人民共和国网络安全法》为我国网络空间治理提供了基本法律框架，但针对民航领域的具体实施细则仍有待完善。为此，可借鉴欧盟《指令 2.0》的立法经验与技术标准，构建清晰完备的民航网络安全术语体系，明确网络安全义务责任主体的分类与权责边界，并依托《网络安全法》进一步细化航空领域的网络安全管理要求。同时，结合我国网络安全等级保护制度，优化安全事件报告与处置机制，提升响应效率。通过系统性立法设计与制度衔接，完善我国民航网络安全法律体系，全面提升民航业的网络安全治理水平。

参考文献：

[1]STERNSTEIN A. Exclusive:FAA computer systems hit by cyberattack earlier this year[EB/OL]. (2015-04-6)[2024-10-05]. https://www.nextgov.com/cybersecurity/2015/04/faa-computer-systems-hit-cyberattack-earlier-year/109384/.

[2]KHARPAL A. Hack attack leaves 1,400 airline passengers grounded[EB/OL]. (2015-06-22)[2024-10-05]. https://www.cnbc.com/2015/06/22/hack-attack-leaves-1400-passengers-of-polish-airline-lot-grounded.html.

[3]DEARDEN L. Ukraine cyber attack:Chaos as national bank,state power provider and airports hit by hackers[EB/OL]. (2017-06-27)[2024-10-05]. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html.

[4]新华社.习近平出席全国网络安全和信息化工作会议并发表重要讲话[EB/OL].(2018-04-21)[2024-10-5]. https://www.gov.cn/xinwen/2018-04/21/content_5284783.htm.

[5]European Commission et,al. Study to support the review of directive(EU)2016/1148 concerning measures for a high common level of security of network and information systems across the Union(NIS Directive),No. 2020-665-Final study report.[EB/OL].(2021)[2024-10-05]. https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1/language-en.

[6]王春晖.《网络安全法》六大法律制度解析[J].南京邮电大学学报(自然科学版),2017(1):1-13.

[7]王朝梁.民航视角下网络信息安全保护的法律对策研究[J].中国政法大学学报,2017(5):66-76.

[8]陈金钊.法律定义的意义诠释[J].江海学刊,2020(4):143-152.

The development and inspiration of EU civil aviation network security legislation

—Taking the EU's *Network and Information System Security Directive 2.0* as an example

XIE Xiaodan

(*School of International Law, East China University of Political Science and Law, Shanghai* 200042, *China*)

Abstract: In order to deal with network threats and establish an integrated EU network security system, the EU issued *Directive 2016/1148* in 2016. However, due to differences and conflicts in practices among the EU member countries, the directive has not achieved the desired implementation effect. In order to eliminate differences and adapt to new changes in network threats, the EU issued the *Network Security and Information Systems Directive 2.0* in December 2022, which reformed some provisions of the former directive, including three types of civil aviation entities under the jurisdiction of "basic entities", and stipulated measures for network security, risk management and obligations for reporting network threats and incidents. *The Cybersecurity Law of the People's Republic of China* provides strategic guidance and legal basis for China's network security work, but lacks specific rules in the field of civil aviation. China can promote the development and improvement of the civil aviation network security legislation by building a comprehensive terminology system for civil aviation network security, standardizing the subjects of civil aviation obligations, refining civil aviation network security management measures, and improving the obligations of reporting network security incidents with the reference to the EU's *Network Security and Information Systems Directive 2.0*.

Keywords: civil aviation; network security; the EU's *Network Security and Information Systems Directive 2.0*; cybersecurity law; network and information system

(责任编辑:周新颜)

引用格式　解晓丹.欧盟民航网络安全立法的发展与启示:以欧盟《网络与信息系统安全指令 2.0 版》为例[J].山东航空学院学报,2025,42(1):60-67.

XIE X D. The development and inspiration of EU civil aviation network security legislation: Taking the EU's *Network and Information System Security Directive 2.0* as an example[J]. Journal of Shandong University of Aeronautics, 2025, 42(1): 60-67.