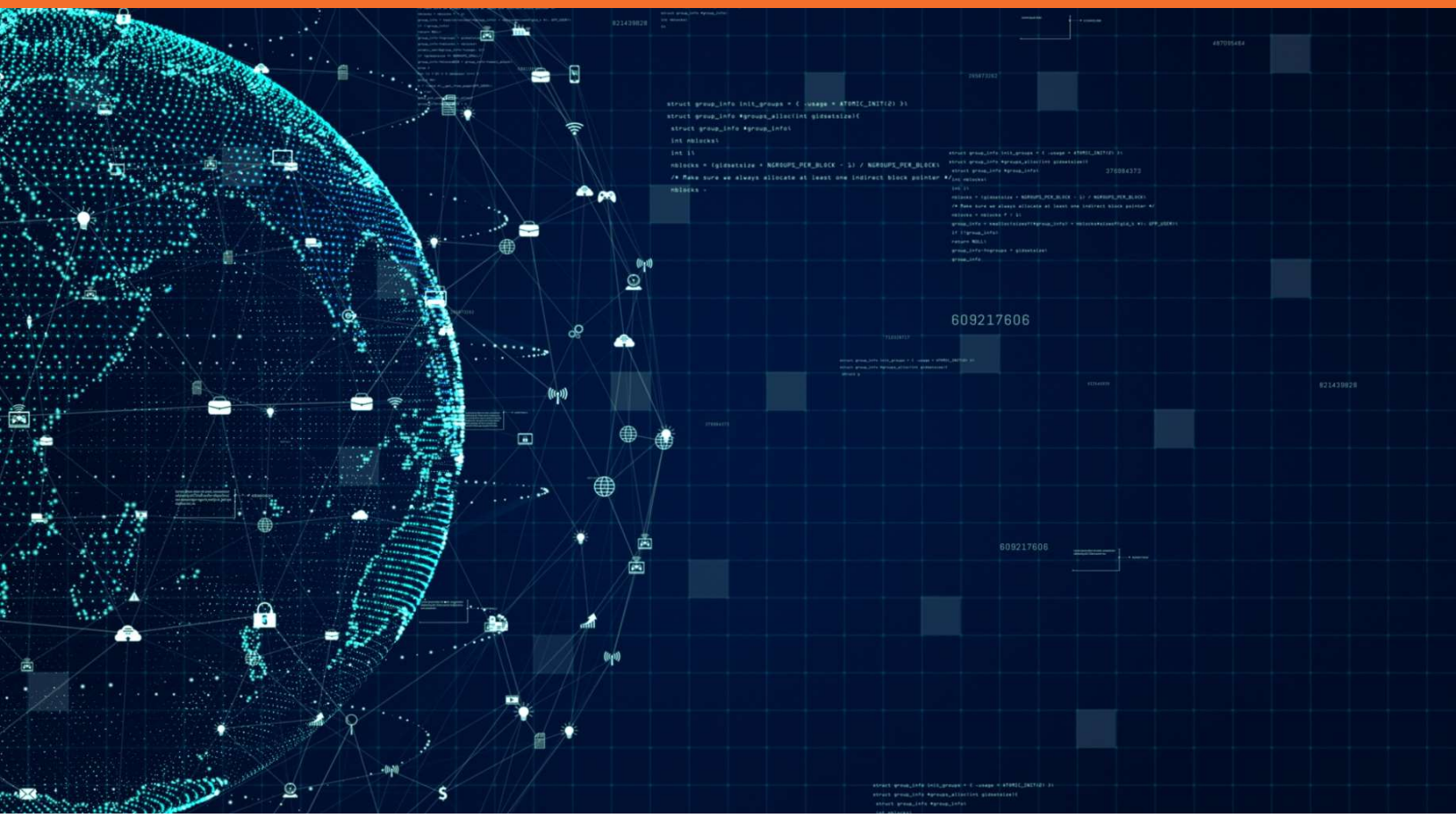
ICAO

SECURITY AND FACILITATION

网 络 信 息 共 享



经秘书长授权出版
2024 年，第 1 版
国 际 民 用 航 空 组 织

目录

缩略语

ANSP	空中航行服务提供者
CAA	民用航空局
CERT	计算机应急响应小组
CIShP	网络信息共享政策
CSIRT	网络安全事件响应小组
CTI	网络威胁情报
FIRST	事件响应和安全小组论坛
ICAO	国际民用航空组织
IoC	危害指标
IPR	知识产权
ISAC	信息共享和分析中心
ISMS	信息安全管理系统
IT	信息技术
OSINF	开源信息
OSINT	开源情报
SOC	安全运行中心
TLP	交通信号灯协议
TTP	战术、技术和程序
UAS	无人航空器系统

执行摘要

在航空安全和航空安保领域确立的最佳做法表明信息共享的重要性及其在减少对民用航空的威胁和风险方面的作用。网络信息共享具有同等的重要性。

网络信息共享对于管理民用航空的网络风险至关重要。它通过促进合作和信任来培养强而有力的网络安全文化。它还支持态势感知、运行和战术性网络风险管理以及战略规划。

本文件为各国和行业利害攸关方制定网络信息共享计划提供指导，包括提供有关制定政策、资源和实际步骤的建议，以实施和不断改进共享做法。

本文件还介绍了航空业共享网络信息的先决条件，列出了可以共享的各种类型的网络信息。此外还讨论了网络信息共享的分析和保证方面的问题，强调需要评估信息来源的信任度和信息的可信度。

本文件取代了先前国际民航组织发布的关于民用航空中使用交通信号灯协议（TLP）的指导。它根据最新的 TLP 标准、共享的信息类型、共享信息的日期/时间和接收者（例如国家机构、运营人、服务提供者）提供了航空业网络信息共享的规则。

总体而言，这份文件强调在民航领域共享各种类型网络信息的重要性，同时考虑进行分析、保证和适当标记，以便在相关利害攸关方之间有效传播信息。

这份指导符合国际民航组织（ICAO）的《航空网络安全战略》[1]及其相关的《网络安全行动计划》，[2]并响应了网络信息共享的需求。这份文件中的信息与《航空安保手册》（Doc 8973 号文件-限制发行）和《安全管理手册》（Doc 9859 号文件）所载的国际民航组织航空安全和航空安保信息共享指导中的一般性原则保持一致。

[1] https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-Strategy.aspx。
[2] https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx。

定义

保证 有计划、有系统地采取必要行动，以充分相信产品或流程能够满足特定要求。

攻击媒介 攻击者用来发起攻击的访问手段。

认证 验证个人、用户、程序、流程、系统或设备的声称身份的措施。

可用性 一种属性，即经授权的个人、用户、程序、流程、系统或设备可根据需求进行访问和使用。

航空网络安全 技术、控制和措施、流程、程序和做法的集合，旨在确保网络资产的保密性、完好性、可用性以及整体保护和复原能力，使其免受攻击、损害、破坏、干扰、未经授权的访问和/或利用。

保密 一种属性，即不向未经授权的个人、用户、程序、流程、系统或设备提供或披露资产。

网络资产 在业务、运行、航空安全、航空安保、效率和/或能力方面具有价值的数字和实物项目，如系统、信息、数据、网络、设备、软件、硬件、流程、固件、相关/经认证人员和其他电子资源。

网络攻击 故意使用电子手段干扰、篡改、破坏或未经授权地访问网络资产。

网络活动 网络或系统中任何可观察的现象。

网络事件 对航空安全、航空安保、效率和/或能力造成不利影响的单一或一系列网络活动。

网络风险缓解 旨在降低与特定网络威胁或漏洞相关的网络风险的安全控制措施，同时虑及其对航空安全、航空安保、效率和/或能力的影响。

网络复原力 网络资产在不利条件或压力下保持关键功能并从那些不利条件中恢复的能力。

网络风险 网络活动可能导致意外结果。

网络风险评估 网络风险识别、分析和评估的持续过程。

网络风险管理 根据风险评估识别、缓解、处理和监控网络威胁和风险的持续过程。

网络威胁 任何可能对航空安全、航空安保、效率和/或能力产生不利影响的潜在网络活动。

信息安全 维护信息的保密性、完好性和可用性。

信息共享 一个实体向一个或多个其他实体提供信息以便基于风险做出决策并促进最佳做法的过程。

完好性 一项资产的准确性和完整性属性，它支持资产宣称的状态。

严重性 对一个威胁条件的不利影响程度的定性表示。

威胁行为者 对影响（或有可能影响）一个组织或系统的事件负有部分或全部责任的实体。

1. 引言

1.1 网络信息共享的理由

信息共享对于支持航空网络风险管理至关重要。在当今互联互通的世界中，网络威胁对民航部门构成重大风险。网络攻击可以针对从空中交通管理系统到乘客数据系统的航空系统的任何方面，可能导致运营中断，并可能危及乘客安全和安保。因此，有效的网络风险管理需要一种协作方法，在利害攸关方之间共享信息。

从航空安全和航空安保中汲取的教训着重表明，信息共享文化将大大降低恶意行为者对民用航空构成的风险。在航空领域，信息共享已被证实为管理航空安全和安保风险的宝贵工具。同样的原则也适用于航空网络安全。通过共享网络信息，利害攸关方可以更好地了解它们面临的网络威胁、查明漏洞并采取适当措施防止或缓解针对民用航空的网络攻击。

信息共享也是强而有力的网络安全文化的一个重要方面。强有力的网络安全文化支持有效识别和应对网络威胁。信息共享是这种文化不可或缺的一部分，因为它促进了利害攸关方之间的透明度、协作和信任。有效的网络信息共享可确保所有利害攸关方都拥有必要的投入，以做出明智的决策、采取适当的行动、减轻网络威胁和/或应对网络事件并从中恢复。

网络信息并不仅限于可采取行动的针对网络的信息，它还包括任何可能对民用航空网络风险产生影响的情报。网络信息共享不只限于针对网络的情报。它还包括任何有助于查明和缓解民航部门网络风险的相关信息。例如，有关实体安全漏洞、内部威胁、地缘政治背景、技术或供应链漏洞的信息也可以帮助利害攸关方更好地了解和缓解网络威胁和风险。

网络信息共享为以下活动提供支持：

- 建立航空网络安全能力的**战略规划**。通过共享信息，利害攸关方可以查明其网络安全能力的差距，并制定适当的战略来提高其网络复原力。战略规划确保航空部门始终受到保护并能抵御网络威胁，并确保利害攸关方做好应对潜在网络事件并从中恢复的准备。
- 在日常运营和网络事件期间保持**态势感知**。通过共享网络信息，利害攸关方可以更好地了解其网络安全态势、网络威胁形势及其系统中的潜在漏洞（弱点）。这使利害攸关方能够查明潜在风险并采取适当措施防止或缓解网络事件的影响。
- 在预测和应对网络威胁时进行**运营和战术性网络风险管理**。通过共享信息，利害攸关方可以查明网络威胁并制定适当的风险管理战略。
- 网络事件期间的**危机管理**，其中有效的信息共享使利害攸关方能协调其应对办法并采取适当措施减轻事件的影响。

必须承认，有效的信息共享以参与者之间的信任为基础。这份指导文件旨在支持建立必要的信任，以鼓励一组参与者克服他们共享信息时自然存在的犹豫。这涉及建立一套共享小组内每个人都理解、同意和遵守的共同规则和程序。就共享哪些网络信息、如何共享以及分发方法达成共识将有助于参与者之间有效地共享信息。

这份指导文件是对国际民航组织航空网络安全整体工作的补充。它支持国际民航组织《航空网络安全战略》支柱 5（信息共享）和《网络安全行动计划》项目 CyAP 5.1，后者要求国际民航组织制定网络信息共享的指导文件。

本文件整合并取代了之前发布的国际民航组织关于在民航中使用交通信号灯协议（TLP）的独立指导材料。本文件包含了关于使用 FIRST（事件响应和安全小组论坛）开发的 TLP 标准更新版本 2.0[3]作为民航网络信息共享手段的指南。

1.2 网络信息共享的背景

在解决网络信息共享之前，必须先解决整个网络情报生命周期的问题。

网络情报生命周期是情报分析领域使用的一个基本迭代流程。这个周期中的每个步骤都发挥着关键作用，用以确保信息从原始数据转化为有意义的情报，使其能支持决策、增强网络安全并支持各种组织战略目标。

信息共享（在下图 1 中也称为“传播”）是网络情报生命周期的一部分，其中包括以下各个步骤：

1. 规划和指导：收集和分析网络信息的第一步是规划和指导这个进程。这涉及确立收集和分析工作的目标、决定其范围和规模以及确定需要参与其中的利害攸关方。规划和指导还涉及制定收集和分析信息的政策和程序，以及确立参与不同步骤的人员的角色和责任。

2. 收集：第二步是实际收集网络信息。这涉及收集来自各种来源的数据（见第 3 节）。收集可以手动完成，也可以通过自动化流程完成。必须确保收集的数据具有相关性、准确和及时。

3. 处理：第三步是处理收集到的信息。这涉及将收集到的数据转换为可用格式，对其进行分析，并查明可能表明存在网络威胁的模式或异常。此步骤可以利用数据处理工具、算法和其他分析技术来帮助识别潜在的网络威胁或漏洞等。处理过程还涉及确定信息的重要性和紧迫性，并相应地确定做出响应的优先级别。

[3] https://www.first.org/tlp/。

4. 分析和制作：第四步是根据处理后的数据进行分析和制作报告。例如，这涉及判读数据、识别模式或趋势以及确定对航空系统造成的网络风险。如果信息的质量和详细程度不足以对其进行分析，则可能导致弃用这个信息。分析人员利用他们的知识和经验来理解数据，并生成与目标受众相关的准确且可操作的情报报告。分析和制作步骤还可能包括编制缓解或预防网络威胁的建议。

5. 传播（网络信息共享）和反馈：最后一步是将情报报告传播给相关利害攸关方。这可以包括与内部利害攸关方（例如信息技术（IT）小组、网络安全小组和/或航空安全/安保小组）以及外部利害攸关方（例如其他航空组织或国家机构）共享网络信息。信息的传播应确保及时和安全地共享网络信息，并使利害攸关方具有就其采取行动所需的背景和理解。有效的传播有助于在民航领域建立网络信息共享文化，并使利害攸关方能够采取可以预防或缓解网络威胁等诸如此类的适当行动。

在此步骤中还收集反馈意见，以便用来评估网络情报生命周期的有效性和相关性，其目的是在未来的迭代中予以增强。

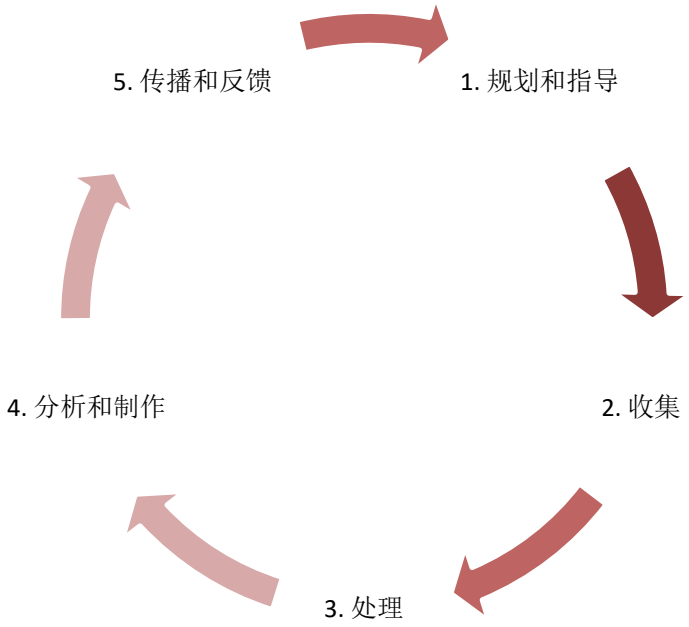


图 1　网络情报生命周期

2. 网络信息共享政策（CIShP）

本节提供如何在机构层面（例如在航空利害攸关方之间）制定和实施网络信息共享政策的指导。

各国也可使用这项指导制定其网络信息共享计划。然而，值得注意的是，国家网络信息共享计划可能是跨部门的，并不特定于航空。

2.1 网络信息共享政策（CIShP）

CIShP 应确定：

- 网络信息共享的理由；
- 适用范围、背景和限制（例如，网络信息来源、与知识产权（IPR）相关的限制、隐私法）；
- 机构内网络信息共享社区的成员及其各自的责任；
- 基于信息分类/类别规则并虑及相关监管和法律要求的机构内外网络信息分发规则（包括进一步分发[4]）；
- 操作程序：
  - 信息收集；
  - 必要时进行去标识化；
  - 内容验证；和
  - 分发；和
- CIShP 的审查周期和文件控制（即记录重大变更和验证程序）。

CIShP 应由机构作为信息安全管理系统（ISMS）[5]的一部分加以批准。它应定期（例如每年）加以审查，在政策发生任何重大改变或发生任何网络事件后进行审查，以汲取相关的教训。

2.2 监管和合同要求[6]

CIShP 应遵守与网络信息共享相关的所有适用法规和现有协议，例如：

- 跨部门的国家、地区和/或国际法规。
- 航空特定的国家、地区和/或国际法规。
- 与国家和/或国际信息共享和分析中心（ISAC）以及计算机应急响应小组/网络安全事件响应小组（CERT/CSIRT）达成的协议（例如，航空信息共享和分析中心、欧洲空中交通管理计算机应急响应小组（EATM-CERT）、国家计算机应急响应小组/网络安全事件响应小组）。

[4] 本文件第 5 节讨论进一步信息共享。
[5] ISO 27001，第 A.5.14 章（信息传输）。
[6] 其他信息（跨部门）参见：
NIST.SP.800-150 – 网络威胁信息共享指导。
ENISA 网络安全信息共享：监管和非监管方法概述。
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive。

2.3 资源

机构应查明确保正确实施 CIShP 所需的资源，包括：

- 人力资源：利用现有的网络安全小组，如安全行动中心（SOC）小组，并根据需要雇用新人员；
- 技术资源：网站、电邮、电话、短信以及安全和/或可信的共享平台；和
- 财政资源：与采购和/或开发系统、人力资源培训等相关的成本。

2.4 实施

CIShP 的实施包括以下阶段：

- 范围界定：确定信息来源和要通过 CIShP 共享的网络信息；
- 确定用于网络信息共享的工具；
- 确定网络信息共享网的联络点（POC）并制定维护 POC 信息的流程；
- 测试网络信息共享的系统和流程，并根据需要对其进行调整；
- 启动网络信息共享方案（上线）；
- 持续监测和控制；和
- 持续审查和改进。

3. 管理网络信息及其共享

3.1 网络信息类型

以下网络信息可以共享。

网络情报

- **网络威胁情报（CTI）：**它包括网络威胁形势、黑客攻击倾向情报等。
  - **战略性：**战略性信息可帮助机构了解网络威胁的类型以及攻击者的能力和动机。
    - 支持对恶意网络威胁的意图和能力形成总体概览。
    - 为决策提供信息和/或提供预警。
    - 它可以包含趋势（例如目标、攻击者的行为）、统计数据、网络威胁相关信息（例如高级持续性威胁（APT）、网络事件报告、政策文件、白皮书/研究论文）等。
    - 战略性 CTI 的一个例子是一份有关国家关键基础设施面临的新兴网络威胁的综合报告，概述了潜在的漏洞和攻击媒介。该报告通常由高层决策者用来制定长期网络安全政策和战略。
  - **运行性：**
    - 提供网络事件背景，使捍卫者能够识别任何可能的危险。
    - 允许识别网络事件对运行的潜在影响（例如战术、技术和程序（TTP）、动机、影响、时间）。
    - 帮助分配资源和设定任务的优先级别。
    - 运行性 CTI 的一个例子是关于针对航空的持续网络钓鱼活动的信息。这包括威胁行为者使用的战术、技术和程序（TTP）等的详细信息。这些信息对于安全行动小组检测和应对即时网络威胁非常有价值。
  - **战术性：**机构为帮助主动构建能够抵御攻击的安全态势而使用的情报（例如危害指标（IoC）、TTPs、漏洞）。
    - 战术性 CTI 的一个例子是与特定恶意软件变体相关的危害指标。这包括特定的 IP 地址、文件哈希值和与恶意软件相关的行为模式。这些战术性信息被一线网络安全分析人员用来实时识别和缓解网络威胁。
- **危害指标（IoC）：**IoC 是恶意 IP 地址、恶意网址（URL）、恶意域名或恶意软件哈希值等。
  - 共享此信息将有助于接收方更好地保护其系统/服务。
  - 共享 IoC 时，无需披露谁发现了它们。
- **战术、技术和程序（TTP）：**TTP 是黑客使用的攻击场景和首选方法。[7]

[7] MITRE ATT&CK 已经开发并维护了 TTP 分类法，可在其网站找到：https://attack.mitre.org/。

- **漏洞：**
  - **作为网络资产的用户：**要共享的网络信息主要与发现漏洞的网络资产（例如硬件、软件、服务、协议、标准）有关。与网络资产用户身份相关的信息不宜共享。
    - 可以与他人共享此信息以帮助他们保护自己。
    - 无需进一步披露谁发现了漏洞。
    - 关于负责任地披露漏洞，机构的漏洞管理方案可以提出“名人堂”或类似流程，以表彰研究人员在查明漏洞方面的贡献。
  - **作为网络资产的拥有者：**网络资产的拥有者应与资产的用户共享漏洞信息。
    - 网络资产的拥有者还应提出补丁/修复方案。
    - 最佳做法包括与 CERT/CSIRT（国家或部门的）共享这些漏洞，以支持他们应对与相关网络资产有关的任何网络事件。
  - 在如何处理共享漏洞相关信息方面，可以考虑在潜在、已确认和已被利用的漏洞之间做区分。

网络事件报告

- 载有对机构产生影响的网络事件的信息。
- 网络事件报告应尽可能列入以下信息：摘要、类型、发生的确切日期和时间、发生地点、持续时间、时间顺序（即事件发生顺序）、IoC、TTP、背景、漏洞、影响（安全、安保、效率、能力、业务、财务、声誉）、严重性、动机、目标、威胁行为者、受影响的服务和机构等。
- 一般而言，提供的信息越多，报告就越具有可操作性。

网络风险缓解

- 载有关于以下方法的信息：
  - 修复漏洞；
  - 缓解网络威胁；和
  - 应对网络事件并从中恢复。
- 此类信息的常见形式包括解决漏洞的补丁、阻止漏洞被利用的防病毒更新软件以及清除网络中恶意行为者的指示。

态势感知

- 包含为决策者提供关于被利用的漏洞、主动威胁和网络攻击的可能必要的实时遥测信息，以应对网络事件。
- 它还可能包含有关攻击目标以及关键公共或私人计算机网络状态的信息。

最佳做法

- 包含与软件和服务的开发和交付方式相关的信息，例如安全控制、开发和事件响应做法以及软件修补或有效性和衡量指标。

3.2 网络信息的发送者、接收者和来源

- 共享网络信息需要有信息发送者、信息接收者和信息来源（如果信息不是来自发送者）。
- 下表包括民用航空中网络信息的发送者、接收者和来源的示例。

发送者/接收者	• 空域用户（例如航空公司、通用航空、无人航空器系统（UAS）运营人） • 空中航行服务提供者（ANSP） • 机场运营人 • 当局（例如民航当局（CAA）） • 航空服务提供者 • 制造商 • 航空和非航空供应链 • 其他
来源	• 上面所列的发送者/接收者 • 航空器（例如无人航空器系统、飞机） • 开源情报（OSINT）来源 • 网络威胁情报（CTI）供应商 • 国际协会和组织（例如航空公司/机场/空中航行服务提供者协会） • 国际/国家/地区航空网络安全中心和航空计算机应急响应小组/信息共享和分析中心（CERT/ISAC） • 其他

- 附录 A 包括可在不同航空利害攸关方之间推荐共享的不同类型的网络信息。

3.3 作为发送者对要共享的网络信息进行评估、分析和附加 TLP 标记

3.3.1 评估和分析

在共享网络信息之前，发送者应进行分析，以便：

- 评估来源的可信度和可靠性（见 3.3.1.1 以及附录 B 和 D）；
- 分析信息的合理性/可信度（见 3.3.1.2 以及附录 C 和 D）；和
- 分析信息对其机构、信息共享社区（接收机构）和航空生态系统的相关性。

这个步骤对于网络信息共享至关重要。没有它，信息将成为一堆没有内涵的数据/发现。

在进行上述分析时，重要的是要记住：

- 不同的分析问题需要不同的方法；和
- 分析人员应意识到他们的内在偏见，并尽可能努力克服这些偏见，使用适当的方法和工具进行客观分析。

为了说明网络信息评估和分析的作用，下面图 2 和图 3 描述了开源信息和开源情报之间的区别，其中至为明显的是，如果在传播前对信息进行适当的分析和保证，信息的可用性就大大提高。

- **OSINF（开源信息）**，收集的信息按原样共享。

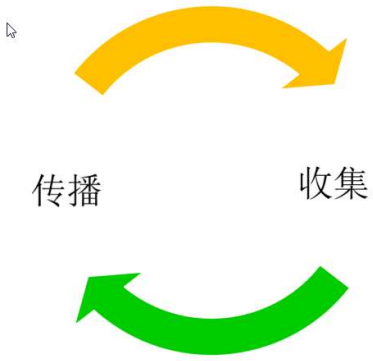


图 2　OSINF - 开源信息

- **OSINT（开源情报）**，信息在收集后将经过以下流程处理。

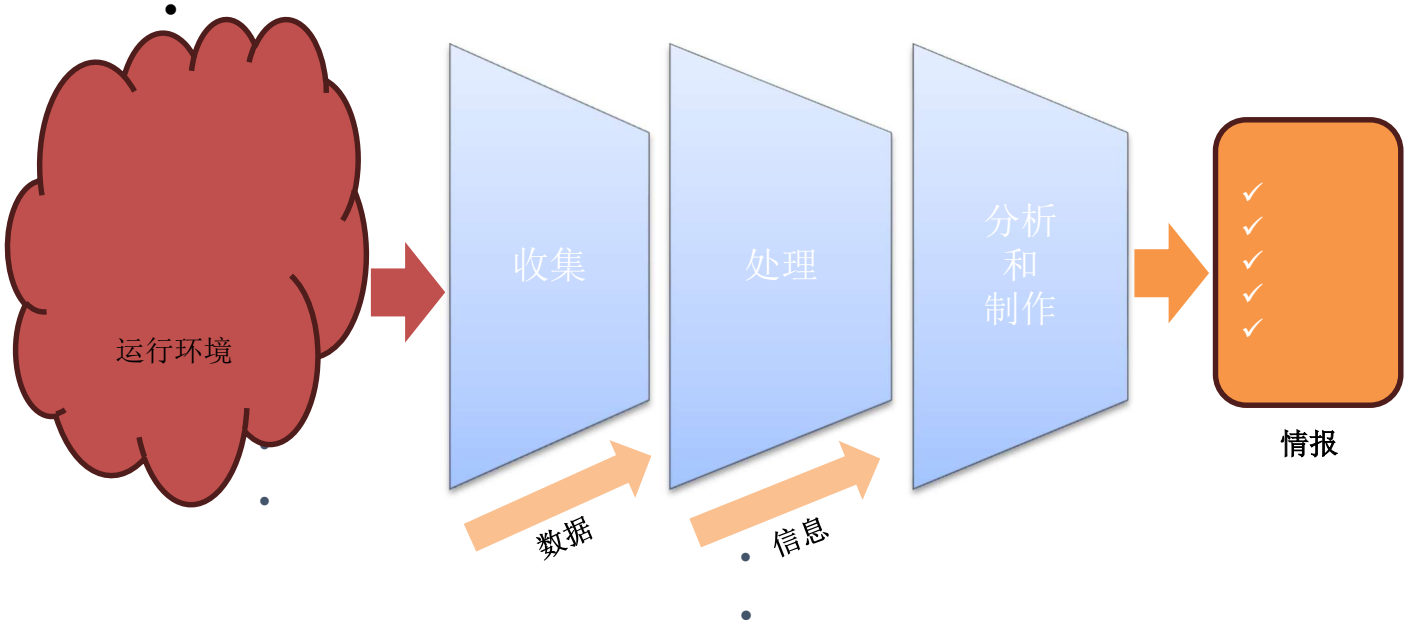


图 3　网络情报制作[8]

3.3.1.1　评估来源的可信度和可靠性

评估网络信息/情报来源的可信度和可靠性水平对于做出明智的决定至关重要。

附录 B 载有一个标准界定框架的示例，并提出一种评估方案来衡量网络信息/情报来源的可信度和可靠性。

附录 B 中使用的权重和评分标准可以调整，以符合机构的具体要求及其风险承受能力。

附录 D 提供了另一个信息信任方案的示例，该方案使用不同的方法评估来源的可靠性和信息的可信度（见下文 3.3.1.2）：《海军法典》（或北约系统）。

网络威胁形势和威胁情报来源随着时间的推移而演变，机构应定期重新评估和更新信任分数。

3.3.1.2　网络信息的合理性/可信度分析

评估网络信息/情报的合理性/可信度水平至关重要。

附录 C 载有一个标准界定框架的示例，并提出一种评估方案来衡量网络信息/情报的合理性和可信度。

附录 C 中使用的权重和评分标准可以调整，以符合机构的具体要求及其风险承受能力。

[8] 改编自联合出版物 2-0，《联合情报》（2013 年）。

随着新的网络威胁信息/情报的出现以及网络威胁形势随着时间的推移而演变，机构应定期重新评估和更新合理性/可信度分数。

附录 D 提供了另一个信息信任方案的示例，该方案使用不同的方法评估来源的可靠性（见上文 3.3.1.1）和信息的可信度：《海军法典》（或北约系统）。

3.3.2 交通信号灯协议（TLP）[9, 10]标记：

3.3.2.1 在航空中使用 TLP

TLP 标准包含五种标记： RED、AMBER、AMBER+STRICT、GREEN 和 CLEAR。

由于 **TLP:CLEAR** 标记不限制通过任何媒介向任何人传播收到的信息，而 **TLP:RED** 标记限于向特定接收者披露信息且完全不会进一步分发，因此本节不讨论这两种标记。需要说明如何在航空环境中应用的三种标记是：

- **TLP:GREEN**
- **TLP:AMBER**
- **TLP:AMBER+STRICT**

TLP:GREEN	- 标有 TLP:GREEN 的信息可在航空界共享。 - TLP:GREEN 信息的接收者可以将其进一步分发给任何航空机构（CAA、ANSP、机场运营人、空域用户、制造商、航空服务提供者等）。 - 还可以将其共享给在航空领域发挥作用的网络安全机构（国家网络安全中心、国家/地区/国际航空 CERT/CSIRT、航空 ISAC 等）。 - 还可以将其共享给使用类似技术（例如与运行或信息技术相关的信息）、受到类似网络威胁或为航空提供服务（例如电信系统或服务、能源系统或服务）的非航空机构。这些非航空机构可以是其他部门的行为者（例如运营人、主管部门、制造商）或网络相关机构（国家网络安全中心、其他部门的相关 CERT/CSIRT、其他部门的 ISAC）。

[9] 交通信号灯协议（TLP）是 FIRST（事件响应和安全小组论坛）开发的标准，用于便利与适当的受众共享信息。本文件提供了有关使用 TLP 标准 2.0 版的指导材料，它可通过以下链接找到：https://www.first.org/tlp/。

[10] 本文件中的指导取代了国际民航组织 2021 年发布的“交通信号灯协议指南”。

TLP:AMBER	- 标有 TLP:AMBER 的信息可在接收者及其客户的机构内**按需要**共享。
	- 尽管机构的含义很简单，但在航空领域，具有**按需要**知晓的“客户”的含义应说明如下：
	  ○ 民航当局可以共享此类信息：
	  ▪ 在其国内与以下机构共享：
	  • 国家航空利害攸关方；
	  • 国家网络安全中心；和
	  • 国家航空 CERT/CSIRT 和 ISAC。
	  ▪ 在其国外与以下机构共享：
	  • 其他民航当局；和
	  • 国家/地区/国际航空 CERT/CSIRT 和 ISAC。
	  ○ 航空利害攸关方（空中航行服务提供者、机场运营人、空域用户、航空服务提供者）可以与以下机构共享此类信息：
	  ▪ 其国家民航当局；
	  ▪ 支持其提供服务的机构；
	  ▪ 国家/地区/国际航空 CERT/CSIRT 和 ISAC；和
	  ▪ 其乘客以外的客户（例如旅行社、免税店）。
	  ○ 制造商可以与以下机构共享此类信息：
	  ▪ 国家民航当局；
	  ▪ 他们的客户（例如航空公司、机场）；
	  ▪ 国家/地区/国际航空 CERT/CSIRT 和 ISAC；和
	  ▪ 他们的分包商。

TLP:AMBER+STRICT	- 标有 TLP:AMBER+STRICT 的信息只可以在接收者机构内**按需要**共享。

3.3.2.2 对不同网络信息建议附加的 TLP 标记

建议在为航空目的标记网络信息时使用以下准则。某些考虑因素可能会导致偏离以下建议，包括但不限于：

- TLP 标记可能会随着时间的推移而演变：网络信息在首次共享时可能会以更严格的标记标示，但随后其标记可能会随着时间的推移而降级，因为与信息相关的风险已随着更广泛的披露而降低。

- 国家与行业对标记的看法：由于不同的考虑因素（例如国家安全限制），国家与航空利害攸关方可以有不同的规则来标记网络信息。

- 适用于行业的国家限制：一个国家可能对适用于国家关键基础设施的某些类型的信息有特定的标记（例如可疑 IP 地址等 IoC 的初始披露）。

网络情报

- **网络威胁情报（CTI）：**
  - **战略性：**取决于战略性 CTI 和受众的性质（例如董事会（BoD）、C 级、CTI 分析人员、蓝队）
    - **TLP:RED**：针对机构的特定网络威胁的具体且非常敏感的情报。需要让有限数量的特定决策者知晓。
    - **TLP:AMBER**：高级管理层、董事会成员或决策委员会成员需要知晓针对机构、与航空相关（例如供应链、关联的利害攸关方）和/或与国家关键基础设施相关的特定网络威胁。
    - **TLP:GREEN**：应与社区共享的情报，以确保其得到广泛了解并就此采取行动（例如政策文件、白皮书、趋势、统计数据）。
  - **运行性：**
    - **TLP:RED**：适用于需要根据针对相关航空利害攸关方或国家关键基础设施（例如供应链、关联的利害攸关方）的特定网络威胁或事件的特定情报采取行动的特定操作、技术和安全人员。
    - **TLP:AMBER**：适用于需要了解针对机构或与航空或国家关键基础设施相关的特定网络威胁或事件的操作、技术和安全人员。
    - **TLP:GREEN**：应与社区共享的情报，以确保其得到广泛了解并就此采取行动。
  - **战术性：**
    - **TLP:RED**：适用于需要根据针对机构的特定网络威胁或需要知晓正在发生的网络事件的特定安全和技术人员。
    - **TLP:AMBER**：适用于需要知晓针对机构或与航空或国家关键基础设施相关的网络威胁或正在发生的网络事件或漏洞的安全和技术人员。
    - **TLP:GREEN**：应与社区共享的情报，以确保对其得到广泛了解并就此采取行动。

- **IoC：TLP:GREEN**
- **TTP：TLP:GREEN**
- 漏洞：
  - 已被利用的漏洞：**TLP:RED**
  - 已被确认的漏洞（有或无补丁）：**TLP:AMBER**
  - 未打补丁的潜在漏洞：**TLP:AMBER**
  - 已打补丁的潜在漏洞：**TLP:GREEN**

网络事件报告

- 没有建议，因为这取决于事件的性质、背景和时间（即网络事件和信息共享之间的时间）。**TLP:CLEAR**可能在早期阶段被排除，但一段时间后可能会适用。

3.4 作为接收者对信息进行评估和分析

网络信息的接收者应分析收到的信息，以确保其：

1. 可信/有保证/优质：对网络信息的信任程度[11]可能不足以考虑该信息是否应触发接收者采取某些行动。
2. **相关性：**相关性的一个例子是，接收者无法根据信息采取行动（例如，不需要知道），而该信息与机构中的其他人员相关。如果收到的信息是 **TLP:RED**，这可能会成为一种障碍。在这种情况下，接收者应与发送者联系，要么征求发送者的同意，通过接收标记级别较低的信息将信息转发给相关接收者，要么为发送者提供机构中的另一个联系人来接收 **TLP:RED** 级别的信息。
3. **可操作性：**TLP 标记可能会阻止接收者根据信息采取行动，这需要发送者和接收者进一步讨论，以便能根据收到的信息采取行动。例如：
   - 信息标记为 **TLP:RED，**而且接收者需要与机构中的其他人联系以便对信息采取行动，但相关人员尚未收到相同的信息。
   - 信息是 **TLP:AMBER+STRICT** 而且接收者需要根据共享的内容与其他机构联系采取行动。

分析还应包括以下活动：

- 接收者应将收到的网络信息与可用的情报相结合（例如，与其他信息相关联和/或加以补充）。这将有助于提高或降低对该信息的信任程度。
- 接收者应将信息与其职责联系起来，这将解决信息在政治、战略、运行、技术和/或网络安全背景下对接收者的意义方面的问题。

[11] 见 3.3.1.1、3.3.1.2 和附录 B、C 和 D。

3.5 各方之间的信任关系

信任是一个动态且多方面的概念，对于敏感信息的安全共享和交换至关重要。它不是绝对的标准，而是一个根据背景、关系和行为而变化的相对标准。

在发送方和接收方之间建立信任关系对于有效的网络信息共享至关重要。

与非传统合作伙伴或利害攸关方建立信任关系也可能是必要的。应确定主动和/或被动网络信息共享的关键方，以确保及时和相关的传播。

可以与各种合作伙伴和利害攸关方建立信任关系。信任关系的例子包括：

- 航空业内部：
  - 国家机构之间（国内和/或国际）
  - 从国家机构到航空组织，反之亦然
  - 行业组织之间
  - 从国家机构或航空组织到国际组织（例如国际民航组织），反之亦然
- 与非航空合作伙伴和利害攸关方：
  - 非政府组织
  - 非营利机构
  - 国际组织（例如联合国相关机构）
  - 国际刑事警察组织 – INTERPOL （ICPO–INTERPOL）

建立信任通常需要时间。国家和利害攸关方可以通过以下方式建立、培育和培养信任关系：

- 与志同道合的合作伙伴结盟。
- 定期活动：参加定期会议或研讨会。
- 协议：以下两节提供了有关可以为网络信息共享制定的协议类型指南。

国家和利害攸关方还应考虑建立和维护信任关系所带来的好处（见第 1.1 节）和成本，以证明此类努力所需的投资合理并就此做出决定。考虑因素应包括：

- 时间：建立和发展关系需要投入多少时间。
- 资源：包括人力资源和财政资源。
- 益处：各方从这种关系中得到什么。
- 责任：建立关系给各方带来的潜在损失。
- 维护：还应考虑在时间和资源方面维持关系的持续成本。

维护信任关系涉及以下活动：

- 面对面会议和虚拟会议：举行会议的次数由双方商定。建议根据需要举行会议，面对面会议至少每年举行一次，同时考虑到所涉及人员的级别（高级、中级或技术级别）。
- 主动网络信息共享：根据需要和优先事项频繁共享信息。这些信息可能包括：
  - 可能影响接收者的政策和程序的变更。
  - 产品：现场报告、战略分析等。
  - 原始信息：源代码、日志等。

- 被动网络信息共享：这可能包括共享与应对网络事件相关的信息：

    - 发生网络事件期间：在事件发生过程中实时且持续地共享信息。
    - 网络事件发生后：共享调查结果、根本原因、经验教训等。

当信任要素被打破时，信任关系也可能会终止。可能导致此类结果的行为示例包括：

- 未经授权披露机密信息：意外或故意向未经授权的个人或机构披露可能具有国家安全或专有意义的机密信息。

- 故意共享敏感信息：故意与个人或机构共享敏感安全信息或敏感专有信息，以暴露漏洞或损害可信度，尤其是在公共领域进行此种行为。

3.5.1 正式协议

各方之间的网络信息共享可以通过双边或多边、有约束力或无约束力的协议正式化。

此类协议涉及不同类型的当事方。例如，可以在国家之间、国家机构之间（例如，同一国家的民航当局与国家网络安全机构之间）、不同国家的政府机构之间（例如，不同国家的民航当局之间）、同一国家的国家机构与航空利害攸关方之间、国家机构与另一个国家的行业利害攸关方之间、和/或航空利害攸关方之间制定协议。

附录 E 提供了正式网络信息共享协议中应涵盖的章节的建议列表，以确保共享网络信息的各方有明确的角色和责任，这将对各方今后的信任水平产生积极影响。

3.5.2 非正式协议

非正式协议通常在交换方之间已经建立或具有信任时使用。应谨慎使用这些类型的协议，因为它们对签署方没有法律义务。它们不应成为网络信息共享的主要或唯一机制。

此类协议包括当事方共享信息所需的有限信息，例如：
- 用于共享信息的技术手段；和
- 各自的联系点（个人和小组详细信息）。

在使用非正式协议共享网络信息时，严格且一致地使用 TLP 标记非常重要，以便维护和培养当事方之间现有的信任。

4. 构建、传达和存档共享的网络信息

4.1 构建要共享的网络信息

应根据确定的分类法或通过确定的结构构建网络信息，以确保在共享时具有足够的内涵以及有用且可操作的详细信息。

这是如何构建要共享的网络信息的示例：

- 标题：网络信息的概述说明
- 参考编号：帮助发送者追踪信息
- TLP 标记
- 主要方面，包括但不限于：
    - 类别（例如网络间谍、网络犯罪、信息运作）
    - 类型（例如漏洞、僵尸网络、监视、个人数据、社交媒体、凭证泄露、网络钓鱼、DDoS、恶意软件）
    - 网络威胁级别（例如严重、高、中、低）
    - 领域/部门
    - 信息来源的信任度和可靠性（参见 3.3.1.1）
- 关键要点：解释信息的要点列表
- 摘要
- 归属：可能已被潜在或实际确定为肇事者的威胁行为者
- 影响、目标、受害者等的评估
- 建议接收者采取的行动
- 可操作信息
    - 受影响的网络资产
    - 时间线
    - 危害指标（IoC）
    - 检测规则
    - 战术、技术和程序（TTP）
- 缓解措施
    - 通用缓解措施
    - 特定缓解措施
- 参考材料

4.2 传达网络信息

本节提供有关使用各种媒体共享网络信息的优点和缺点的指导。

4.2.1 电话

这种类型的通信适合用于 TLP:RED 标记的信息，以确保与预期接收该信息的人同步通信。它还有助于传达需要立即采取应对措施的关键信息。

如果使用电话共享网络信息，建议考虑采取控制措施以确保双方的身份（例如避免 AI 生成的音频注入）。

总体而言，这种媒介的可用性有限（主要用于共享高紧急性和/或 TLP:RED 的网络信息），因此应与其他网络信息共享媒介结合考虑。

4.2.2 纯文本电子邮件

网络信息可以纯文本形式在电子邮件中共享。

使用这种媒介共享网络信息意味着：

- 接收者必须打开电子邮件并阅读信息。
- 需要由 CTI 分析人员分析内容以评估其与接收者的相关性。
- 信息最初将手动处理。

以下是使用纯文本电子邮件共享网络信息的一些限制：

- 这种媒介适合简短和基于文本的内容。
- 某些电子邮件系统可能会阻挡这种电子邮件，因为其中可能包含了 IoC，这会触发 IT 安全控制措施。
- 难以维护最新的电子邮件列表。建议使用个人和通用电子邮件地址。
- 标记为 TLP:RED 的信息不能发送到通用电子邮件（例如 groupmailbox@company.com），而只能发送到个人电子邮件（例如 someone@company.com）。
- 某些类型的电子邮件地址可能不被视为受信任的接收者（例如，托管在商业电子邮件托管服务（如 gmail/hotmail/yahoo/等）上的非专业电子邮件地址）。
- 存在电子邮件冒充的风险。因此，建议使用适当的身份验证方法（例如电子邮件数字签名）来管理该风险。

4.2.3 带有附件的电子邮件

网络信息可以在附于电子邮件的文件中共享。可以使用密码加密附件，然后可通过其他受信任的方式（例如短信、安全消息传递应用程序）将密码发送给接收者。

使用这种媒介共享网络信息意味着：

- 接收者必须打开附件并阅读信息。
- 需要由 CTI 分析人员分析内容以评估其与接收者的相关性。
- 信息最初将手动处理。

以下是使用带有附件的电子邮件共享网络信息的一些限制：

- 存在点击恶意附件的风险 - 因此必须先净化清理附件。
- 某些电子邮件系统会阻挡某些类型的附件（例如压缩文件，如带有扩展名为.zip、.rar 和.7z 的文件）。
- 某些电子邮件系统可能会阻挡对文件的访问，因为其中可能包含了 IoC，这会触发 IT 安全控制措施。
- 附件的大小可能会阻止其通过电子邮件传输。
- 难以维护最新的电子邮件列表。建议使用个人和通用电子邮件地址。
- 标记为 **TLP:RED** 的信息不能发送到通用电子邮件（例如 groupmailbox@company.com），而只能发送到个人电子邮件（例如 someone@company.com）。

4.2.4 私人数据存储库

可以通过访问存储共享信息的私人数据存储库来共享网络信息。

在这种方案中，应制定通知方法，通知接收者有新的网络信息可供访问。

此种通知可以通过电子邮件或其他方式（例如短信、安全通信应用程序）自动完成。

必须保护和维护对数据储存库的访问：

- 应依照数据存储库中的共享信息的敏感度设置安全控制/保护措施。控制措施可以包括数据存储库托管（例如私人/共享服务器、云托管）、访问控制/权限、用户身份验证方法（例如单点登录（SSO）、双/多重身份验证（2FA/MFA））等。
- 应持续维护有权访问数据存储库的组织/个人列表，以确保其时效性和真实性。
- 应向个人帐户提供访问权限（例如读取和写入权限）并进行维护。
- 应记录和分析对数据存储库进行的所有访问和操作。
- 应将数据存储库上发布的网络信息仔细按类别编入文件夹，因为并非所有参与者都具有相同的信息访问权限。此外，由于信息的分类（例如 TLP 标记）会随时间变化（例如，如果类别/TLP 标记降级，则可能会有更多受众可以访问），因此信息需要在文件夹之间移动。随着社区成员数量和数据存储库上共享的信息随着时间推移而增多，这可能会成为一个复杂的过程。

4.2.5 应用程序

各种软件应用程序（开源或商业）可用于共享网络信息（例如 MISP、OpenCTI、CyWare 等）。

为应用程序提供一个通用的注意事项列表是不可能的，因为这取决于应用程序的性质（例如开源或商业）、谁负责开发和更新安全控制措施、访问权限、信息分类（例如通过规则手动或自动分类）、敏感信息存储（例如安全/私人或公共服务器）等。因此，建议在考虑使用应用程序进行网络信息共享时，评估所有这些方面以及其他必要的方面。

在现有应用程序中，附录 F 提供了有关 MISP（开源威胁情报和共享平台）的信息，因为该平台提供了有用的功能，可以支持航空业共享网络信息的努力。

4.3 存档网络信息

出于记录保存和质量控制的目的，发送者和接收者都应将共享的网络信息存档。

存档信息时应考虑以下方面：

- 规则：应考虑可能适用于信息存档的规则（例如，隐私法及其对特定类型信息存档的要求以及允许该信息在档案中保存的最长时间）。

- 存储媒介：使用何种存储媒介取决于信息的类型。可以使用不同类型的媒介来存档网络信息。例如，网络事件报告可以存储在特定的独立数据库，网络威胁情报报告可以作为文件存储在计算机磁盘等。

- 访问控制和权限：对存档的网络信息的访问应根据谁能访问何种信息的政策来确定。这与信息的 TLP 标记相符（例如，**TLP:AMBER+STRICT** 并不表示机构中的每个人，而只是那些需要知道的人）。

- 本地与远程可访问性：某些网络信息可能不允许从机构外部访问（例如通过内部网），而只能在内部访问。这还包括根据人员的角色和职责确定的访问权限，这些权限可用于审计/保证目的。

- 安全控制/保护措施：根据信息类型，应实施不同级别的安全控制和保护措施。例如，应实施比保护已修补的漏洞更严格的控制措施来保护网络事件报告。

- 相关性：由于事态发展，某些网络信息可能已经过时。例如，机构不再使用的系统的漏洞、与不再存在的地缘政治事件相关的战略网络威胁情报等。

- 可用性：应确定档案的各种类别，以支持信息的持续可用性。例如：
  - “热”：包括存储到文件的未经压缩的最新数据，以便以最佳性能进行检索和处理；
  - “温”：包括略加压缩而存储的数据，以便能在需要时以很好的性能进行检索和处理；
  - “冷”：包括已经存档并已完全压缩的数据，需要手动检索和解压才能使用。

- 保存时间：应根据信息类型考虑已存档的网络信息的保存时间。例如，可以制定存档规则，使 IoC 不超过[X]年。此外，应将删除过时信息的相关操作作为网络信息存档管理流程的一部分来实施。

5. 进一步共享网络信息

5.1 为何要进一步共享网络信息

进一步共享从外部来源收到的网络信息可能是必要的，以确保这些信息被最广泛的需要知道的受众所了解。不过，在进一步共享网络信息之前应给予仔细考虑。

举个例子，一个国家机构从最初发送者那里收到信息，指出该信息只允许与最初发送者有正式协议的实体进一步共享。国家机构作出评估认为，与信息最初发送者没有达成正式协议的其他国家机构需要知道这个信息。在这种情况下，信息接收者应与信息最初发送者联系并征求其同意，以便进一步与需要知道该信息的其他机构共享该信息。

为了确定是否以及与谁进一步共享网络信息，信息接收者应考虑以下因素：

- 进一步共享的限制：是否可以或应该进一步共享此信息？如有疑问（例如怀疑 TLP 标记可能遭到滥用），接收者可以寻求发送者的许可，以进一步共享信息。
- 进一步共享信息的目的和被考虑的接收者的角色。

进一步共享网络信息的目的与期望接收者采取何种行动有关：

- 供参考/知悉：被考虑的接收者需要知道信息，且共享的信息仅供参考。
- 供采取行动：被考虑的接收者需要知道信息，且进一步共享信息是为了接收者采取具体行动。此类行动可以包括：
  - 分配或调动资源以解决特定问题。
  - 分配或调动资源以缓解特定网络威胁或漏洞。
  - 分配或调动资源以协助采取应对措施。

被考虑的接收者的角色可能是决定是否进一步共享网络信息的一个因素。可能有需要知道信息的角色包括：

- **技术专家：**负责监督保护网络、系统、服务、应用程序、IT/OT 基础设施等免遭未经授权访问的专家或技术人员。

- **政策制定者：**起草航空或相关非航空网络安全战略、政策、程序和/或流程供航空利害攸关方实施的人。

- **决策制定者：**批准实施航空或相关非航空网络安全战略、政策、程序和/或流程的高级工作人员。

- **协调员：**负责将共享信息有效地传递给正确人员的网络安全专家或技术人员。

- **航空安全官：**可以进一步确定对航空安全、效率和/或能力产生的可能影响的航空安全专家。

- **航空安保官：**可以进一步确定对航空安保产生的可能影响的航空安保专家。

5.2 进一步共享网络信息的规则

进一步共享网络信息的规则包括许多需要仔细考虑的领域：

- 与其进一步共享信息的机构（例如，国家/航空利害攸关方/非航空利害攸关方、国家/国际实体）。
- 进一步与其共享网络信息的接收者的角色。
- 共享的内容：全部网络信息或其摘录（例如，整份文件或仅有相关段落）。
- 在什么情况下共享信息：主动或被动。
- 共享的频繁程度：常规或根据需要。
- 共享网络信息的原因（例如，供参考或供采取行动）。
- 处理网络信息的方法：所有原始分类和警告都必须保留在适当的通信渠道中（即机密和非机密通信渠道）。
- 进一步共享网络信息时，不能更改其 TLP 标记。

5.3 进一步共享信息的方法和媒介

进一步共享网络信息的方法/媒介应在适当的情况下安全且简单。

实物信息：以硬拷贝形式提供的信息。在将信息送到会议地点和提供硬拷贝之前，应妥善包装（例如，放在文件夹中）并妥善保护（例如，用拉链或锁扣封口的文件夹）。任何处理信息的提醒或警告都应在信息本身或封面上注明（例如，处理敏感安全信息（SSI）[12]的警告通常都列于带有说明的封面页）。

电子信息：第 4.2 节讨论的网络信息共享方式也适用于进一步共享信息。不过，应考虑到与其进一步共享网络信息的预期接收者可能无法访问发送者可以访问的某些电子方式（例如，白名单电子邮件、访问信息所在的门户/存储库）。

各国或机构对处理机密信息都有不同的附加规则。应严格按照适用的规定和程序遵守这些规则。

———————————

[12] 国际民航组织《*航空安保手册*》（Doc 8973 号文件 - 限制发行）第 2.3 节有关处理航空安保敏感信息的指导提供了可用于网络信息共享环境的有用信息。

附录 A
依照信息类型建议在航空领域共享的网络信息

网络情报

- **网络威胁情报（CTI）：**
  - **战略性：**
    - 从国家机构（国家网络安全中心、民航当局等）到国内航空利害攸关方
    - 从国家网络安全中心到航空 CERT/ISAC
    - 从航空 CERT/ISAC 到航空利害攸关方
    - 可信的国家网络安全中心之间
    - 可信的国家之间
  - **运行性：**
    - 从航空利害攸关方到航空利害攸关方
    - 从航空 CERT/ISAC 到航空利害攸关方
    - 从国内航空利害攸关方到国家机构（国家网络安全中心、民航当局等）
  - **战术性：**
    - 从航空利害攸关方到航空利害攸关方
    - 从航空 CERT/ISAC 到航空利害攸关方
    - 从国家网络安全中心到航空 CERT/ISAC
    - 从国家网络安全中心到国内航空利害攸关方
    - 从航空利害攸关方到国家机构（国家网络安全中心、民航当局等）
- **危害指标（IoC）：**
  - 从航空利害攸关方到航空利害攸关方
  - 从航空 CERT/ISAC 到航空利害攸关方
  - 从国家网络安全中心到航空 CERT/ISAC
  - 从国家网络安全中心到国内航空利害攸关方
  - 从国内航空利害攸关方到国家网络安全中心
- **战术、技术和程序（TTP）：**
  - 从航空利害攸关方到航空利害攸关方
  - 从航空 CERT/ISAC 到航空利害攸关方
  - 从国家网络安全中心到航空 CERT/ISAC
  - 从国家网络安全中心到国内航空利害攸关方
  - 从国内航空利害攸关方到国家网络安全中心

- **漏洞：**
  - 从航空利害攸关方到航空利害攸关方
  - 从航空利害攸关方到其供应链提供者
  - 从研究人员到航空 CERT/ISAC
  - 从研究人员到国家机构（国家网络安全中心、民航当局等）
  - 从研究人员到航空利害攸关方
  - 从研究人员到供应链
  - 从航空 CERT/ISAC 到航空利害攸关方
  - 从国家网络安全中心到航空 CERT/ISAC
  - 从国家网络安全中心到国内航空利害攸关方
  - 从国内航空利害攸关方到相关国家机构（国家网络安全中心、民航当局等）

网络事件报告

- 强制性网络事件报告（通过适用的国家法律和/或法规）：
  - 从国内航空利害攸关方到相关国家机构（国家网络安全中心、民航当局等）（针对航空安全和/或安保事件）
  - 从航空利害攸关方到执法机构（针对与欺诈等网络犯罪或隐私法等特定法律相关的特定事件）
  - 从国家到国际民航组织（针对与非法干扰行为相关的网络事件）

- 自愿网络事件报告：
  - 从航空利害攸关方到国家网络安全中心
  - 从航空利害攸关方到航空利害攸关方（特别是如果它们正在互动）
  - 从航空利害攸关方到航空 CERT/ISAC

附录 B
网络信息/情报来源可信度和可靠性的评估和排名框架示例

1. 声誉和记录：
   - 评估信息来源在网络安全社区的历史和声誉。
   - 寻找过去的成功、贡献以及它们在行业机构中的参与。
   - 评估它们在提供准确和及时的网络威胁信息/情报方面的记录。

2. 可信度和专业知识：
   - 评估来源背后的个人或团队的资格、认证和专业知识。
   - 考虑它们在网络威胁信息/情报特定领域的经验。

3. 数据来源和收集方法：
   - 检查信息来源的数据收集方法和来源。
   - 确定它们是否可以访问多样化和可靠的数据源。
   - 评估其数据收集过程的严谨性。

4. 数据共享和协作：
   - 确定信息来源是否与可信的机构或行业同行共享网络威胁信息/情报。
   - 与其他网络安全实体的协作可以提高可信度。

5. 透明度：
   - 评估其报告和方法的透明度。
   - 评估它们是否披露其数据来源、分析技术和更新报告次数。

6. 及时性和准确性：
   - 评估信息来源提供及时和准确的网络威胁信息/情报的能力。
   - 考虑它们在预测和检测网络威胁方面的以往表现。

7. 分析和背景：
   - 分析其网络威胁分析的深度和质量。
   - 评估它们提供有关网络威胁的背景信息的能力，包括归属和潜在影响。

8. 与行业标准符合：
   - 确定信息来源是否遵循网络威胁信息/情报方面的行业标准和最佳做法，例如是否遵守 STIX/TAXII 等框架和通用数据格式。

9. 遵守法律和道德规定：
   - 确保信息来源遵守有关数据收集和共享的法律和道德标准。

为了衡量对网络信息/情报来源的信任程度，可以使用基于上述标准的评分系统。

以下是评估方案的示例。

1. 根据每个标准对机构特定需求和风险状况的重要性对其进行加权。
2. 根据每个标准的等级（例如 1-5）对来源进行评级，其中 5 表示最高信任级别。
3. 通过将每个标准的加权分数相加来计算总体信任分数。分数越高，表示来源越值得信任。

以下是计算总体信任分数的简化示例：

- 声誉和记录： 4/5
- 可信度和专业知识： 5/5
- 数据来源和收集方法： 3/5
- 数据共享和协作： 4/5
- 透明度： 4/5
- 及时性和准确性： 4/5
- 分析和背景： 5/5
- 与行业标准符合： 4/5
- 遵守法律和道德规定： 5/5

总体信息来源信任分数可以是：
(4*0.1) + (5*0.15) + (3*0.1) + (4*0.1) + (4*0.1) + (4*0.1) + (5*0.15) + (4*0.1) + (5*0.1) = **4.30**

— — — — — — — — —

附录 C
网络信息/情报合理性/可信度的评估框架示例

1. 来自多个来源的确证：
   - 评估网络威胁信息/情报是否得到多个独立来源的确证，例如，多个来源报告相同的信息可以增加合理性。

2. 与已知威胁和战术的一致性：
   - 确定网络威胁信息/情报是否与已知的网络威胁、攻击技术和战术一致，例如，出现不一致的情况可能表明合理性较低。

3. 技术细节和证据：
   - 检查是否存在支持网络威胁信息/情报的技术细节和证据，例如，强有力的技术证据会增加合理性。

4. 归属和动机：
   - 评估网络威胁的归属为特定行为者或团体。
   - 考虑这些行为者的动机以及它是否与报告的网络威胁一致。

5. 时机和背景：
   - 分析网络威胁的时机及其在网络安全格局中的背景。
   - 考虑网络威胁是否与当前事件或趋势相符。

6. 历史准确性：
   - 评估信息来源在报告网络威胁方面的历史准确性，例如，拥有持续的准确报告的记录会增加合理性。

7. 同行验证和信任团体：
   - 确定网络威胁信息/情报是否已得到可信的同行或行业团体的验证或认可，例如，如获同行验证可以提高合理性。

8. 危险信号和异常：
   - 寻找网络威胁信息/情报中的危险信号、异常或可疑元素；解决和解释这些问题可以提高合理性。

为了衡量网络信息/情报的合理性/可信度水平，可以使用基于上述标准的评分系统。

以下是评分系统的示例。

1. 根据每个标准对其机构的网络风险评估的重要性和相关性对其进行加权。

2. 根据每个标准的等级（例如 1-5）对威胁情报进行评级，其中 5 表示最高合理级别。

3. 通过将每个标准的加权分数相加来计算总体合理性分数。分数越高，表示威胁情报报告有越高的合理性。

以下是计算总体合理性/可信度分数的简化示例：

- 来自多个来源的确证： 4/5
- 与已知威胁和战术的一致性： 3/5
- 技术细节和证据： 5/5
- 归属和动机： 4/5
- 时机和背景： 4/5
- 历史准确性： 4/5
- 同行验证和信任团体： 4/5
- 危险信号和异常： 3/5

总体合理性/可信度分数可以是：

(4*0.15) + (3*0.15) + (5*0.15) + (4*0.1) + (4*0.15) + (4*0.1) + (4*0.1) + (3*0.1) = **3.90**

———————

附录 D
网络信息信任方案示例

本附录介绍了《海军法典》，[13]这是评估收集到的情报项目的另一个方法示例。

在共享信息时，可以使用该计量表来了解来源的可靠性和信息的可信度。这个方法由两个字符符号（一个字母和一个数字）组成，字母评估来源的可靠性，数字反映评估后对信息的信任程度。

来源的可靠性

来源的可靠性基于对其能力的技术评估，在人为情报来源的情况下，来源的可靠性基于对其历史的评估。如下所示，使用从 A 到 F 的字母符号对来源的可靠性评分。

可靠性代码	可靠性	说明
A	完全可靠	真实性、可信度或能力都毫无疑问；具有完全可靠的历史。
B	通常可靠	对真实性、可信度或能力略有怀疑；历史上大多数情况下都提供有效信息。
C	比较可靠	对真实性、可信度或能力存有疑问，但过去曾提供过有效信息。
D	通常不可靠	对真实性、可信度或能力存有重大疑问，但过去曾提供过有效信息。
E	不可靠	缺乏真实性、可信度和能力；有提供无效信息的历史。
F	无法判断可靠性	不存在评估来源可靠性的基础。

[13] 这个方法的详细信息可查阅《联合条令出版物 2-00：联合行动的情报、反情报和安全支持》（第四版）第 59 页和第 60 页，网址为：https://www.gov.uk/government/publications/jdp-2-00-understanding-and-intelligence-support-to-joint-operations。

信息的可信度

根据可能性和其他来源的证实程度来评估项目的可信度。如下所示，使用从 1 到 6 的数字符号对来源的可信度评分。

可信度分数	可信度	说明
1	经其他来源证实	经其他独立来源证实；本身合乎逻辑；与有关该主题的其他信息一致。
2	大概为真	未经证实；本身合乎逻辑；与有关该主题的其他信息一致。
3	可能为真	未经证实；本身合乎逻辑；与有关该主题的其他一些信息一致。
4	可疑	未经证实；可能但不合逻辑；没有关于该主题的其他信息。
5	不太可能	未经证实；本身不合逻辑；与该主题的其他信息相矛盾。
6	无法判断真实性	没有评估信息有效性的基础。

上面两表可合并为下表。

来源的可靠性		网络信息的可信度	
A	完全可靠	1	经其他来源证实
B	通常可靠	2	大概为真
C	比较可靠	3	可能为真
D	通常不可靠	4	可疑
E	不可靠	5	不太可能
F	无法判断可靠性	6	无法判断真实性

以下是共享的网络信息评级的两个示例：

- C4 的含义是：比较可靠的来源和可疑的信息。
- A1 的含义是：来源完全可靠和信息经其他来源证实。

虽然评估是主观的，但评级提供了一个有用的工具，它可支持网络信息的接收者对网络信息进行他自己的评估和分析。

附录 E
正式网络信息共享协议的建议结构

正式的网络信息共享协议应包括以下各部分：

- ✓ 序言，包括当事方的名称和说明。
- ✓ 定义和缩略语。
- ✓ 范围：说明文件的范围，并参考附录 1，其中涵盖了要共享的网络信息类型。
- ✓ 信息接收者（接收人）的权利和义务。
- ✓ 信息来源：谁将向谁提供何种信息、基于何种来源以及是否需要共享信息来源。
- ✓ 根据现有法律、知识产权、商业机密信息、TLP 标记的定义等，对可以共享哪些信息和与谁共享信息作出限制。
- ✓ 交换的信息的格式和频繁程度。
- ✓ 信息传输方式（如信件、电话、短信、电子邮件、数据存储库等），包括保护和确保数字传输的信息的保密性、完好性和可用性。
- ✓ 质量要求：说明发送者在传输信息之前要执行的操作。它还说明确保共享信息的完好性和质量的方法，例如包括信息的去标识化和/或净化。
- ✓ 存储和记录保存：说明共享信息的归档政策和程序。它还说明了为管控协议的质量和为各当事方之间的关系而应将发送/接收的信息归档保存的最短时间。
- ✓ 费用：说明哪一当事方承担共享信息的费用。建议每一方承担它自己与协议实施相关的费用。
- ✓ 协议的治理和变更管理程序。
- ✓ 与协议相关的信函和通知。
- ✓ 责任：说明各自担负的责任。建议免除发送者与共享信息相关的责任。
- ✓ 个人数据处理：说明如何处理个人数据，包括适用的法律和法规。
- ✓ 争端解决：如何以及根据哪些法律解决与协议相关的争端。建议当事方首先尝试友好解决争端，如果不成功，则在商定的司法管辖范围内通过调解解决。
- ✓ 整份协议和修订：说明协议各部分的优先顺序。
- ✓ 协议生效日期、期限以及续签和终止程序。
- ✓ 授权签名：获当事方授权的人的签名。
- ✓ 附录：
  - 附录 1-需要提供的信息：说明当事方共享的信息类型。
  - 附录 2：TLP 标记的定义，包括对 FIRST TLP 标准的引用。

附录 F
MISP - 开源威胁情报和共享平台

MISP[14]是一个用于共享、存储和关联有针对性网络攻击的危害指标（IoC）以及威胁行为者信息、金融欺诈信息等网络威胁情报的平台。

它是一个免费的开源网络威胁情报和共享平台，允许各机构创建社区来共享信息，例如网络威胁情报、指标、威胁行为者信息或任何可以在 MISP 中存储的网络威胁。

MISP 用户从共同了解现有恶意软件或网络威胁之中获益。MISP 通过创建“社区”来使用。信息共享发生在用户社区内。这个基于信任的平台旨在帮助改进反制措施，以便打击有针对性的网络攻击，以及加强预防行动和检测的实施。

建议各国和航空利害攸关方将 MISP 以及任何同等平台视为共享网络信息的媒介/方法，因为该平台：

- 有助于自动使用收到的信息来更新各种安全系统，例如安全信息和事件管理/安全运行中心（SIEM/SOC）、防火墙、防病毒软件和入侵检测和预防系统/入侵预防系统（IDPS/IPS）；
- 允许快速共享网络信息，因为在应对当前网络事件而共享信息时，时间可能是一个关键因素；
- 当有其他与网络事件相关的网络信息时，允许更新此种网络信息；和
- 所有类型的 TLP 标记信息均可通过 MISP 共享。不过，只有在社区由同意共享此类信息的有限人数组成时，标记为 **TLP:RED** 的信息才会在 MISP 上共享。一般而言，**TLP:RED** 信息不会在 MISP 上共享，而是通过其他方式（例如，电话、短信和电子邮件）共享。

— 完 —

[14] 关于使用 MISP 的进一步信息，参见：https://www.circl.lu/services/misp-malware-information-sharing-platform/。