ACCCF / 应用知识图书馆

12

卷

模式、关系与归因边界

西班牙语版 · 2026

机器人网络、虚假个人资料与媒体损害分析手册

证据保存、时间线、指标、关系图、替代假设与技术报告

分析协调行为，同时不把巧合当作自动化的证据、不把账户关系当作账户归属的证据，也不把不受欢迎的观点当作犯罪证据。

面向分析人员、鉴定人、研究人员、法律团队，以及传播、声誉和合规人员。收集工作仅限于公开或经授权的来源，不包括规避控制、冒充身份或暴露个人。

编辑统筹：Jocsan Laguna · 美洲网络安全与计算机取证委员会

通用技术指南与开放教育材料。不构成法律意见、专家鉴定意见，也不提供未经授权访问系统的指导。示例和数据均为虚构；图示为编辑重构。

目录

所示页码对应 PDF 版。Word 可在打开文档时更新本目录；标题保留内部导航。

前言：许多账户不等于一个人 3

第1章 问题与判定标准 3

- **1.1 需要不同证据支持的论断** 3
- **1.2 假设与证伪** 4

第2章 现场保全 4

- **2.1 可能消失的对象** 4
- **2.2 关系与顺序** 4
- **2.3 隐私与比例原则** 5

第3章 内容与时间线 6

- **3.1 文本、变体与早期来源** 6
- **3.2 时间窗口与频率** 6
- **3.3 链接与参数** 6

第4章 协调行为与假设 7

- **4.1 相互印证的指标** 7
- **4.2 账户年龄、变更与社群** 7
- **4.3 自动化评估** 7

第5章 关系图与基础设施 8

- **5.1 节点不等于个人** 8
- **5.2 域名、IP 与共享服务** 9
- **5.3 归因分级** 9

第6章 媒体损害与报告 9

- **6.1 范围与后果** 9
- **6.2 可复现的技术报告** 10
- **6.3 后续行动** 10

附录A 分析格式 11

- **A.1 账户与内容清单** 11
- **A.2 指标矩阵** 11
- **A.3 报告结构** 12
- **A.4 使用模拟时的记录** 12

附录B 法律框架与最终检查 12

前言：许多账户不等于一个人

十二个个人资料发布相同文本，可能看似一次集中操作，也可能只是一个社群在分享模板、突发新闻或正当倡议。分析首先要避免轻率下结论：描述这些账户做了什么、按什么顺序行动、存在哪些关系，以及哪些其他解释可能产生相同模式。

“机器人”“虚假个人资料”“协调账户”“网络喷子”“账号农场”和“影响力操作”不是同义词。一个账户可以自动化但未参与协调；多个人可以不借助自动化而协调行动；一个个人资料可以使用虚构姓名，但并非整体虚假；一场活动可以包含真实内容，同时采用欺骗性行为。报告应分别定义这些类别并分别加以验证。

分析无需编造标题也能发挥价值。它可以证明，相对于有记录的参照基准，一组账户在文本、时间窗口、链接、顺序和关系方面存在异常共性。共同基础设施可以提供线索，但一个 IP 地址或域名并不能证明所有账户都属于同一个人。归因必须止步于来源所能支持的范围。

> **指导原则**
>
> 先看模式和覆盖范围，再考察替代解释；最后才确定证据实际支持的归因程度。

第1章 问题与判定标准

1.1 需要不同证据支持的论断

应区分五个问题：发布了什么内容、哪些账户参与、表现出什么行为、存在哪些关系，以及谁控制这些账户。前几个问题可以通过帖子和记录回答；协调行为需要比较分析；账户归属则需要另一类来源。如果不加区分，一张美观的图最终会表达超出研究所能支持的结论。

范围包括平台、时段、时区、初始账户、检索词、内容类型、数据来源和排除标准。应记录样本的发现方式：搜索、既有列表、API、导出、推荐来源或手动选择。凭愤怒选择样本会造成样本偏差。如果只截取病毒式传播的帖子，就无法与普通行为进行比较。

论断	所需证据	不得默认得出的结论
内容完全相同	文本、版本、URL、日期和早期来源。	单一作者或统一发布中心。
同时性	时区、可获得的秒级精度和完整顺序。	仅凭时间接近就认定自动化。
协调行为	多项指标和参照比较。	仅凭一次巧合就认定协调。

论断	所需证据	不得默认得出的结论
自动化	技术模式、活动和可用的控制信息。	所有重复行为都是机器人所为。
账户归属	控制记录与法律层面的印证。	仅凭照片、IP 或姓名认定个人身份。
损害	经证实的内容、传播范围、背景和后果。	仅凭展示次数认定全部影响。

1.2 假设与证伪

一个初始假设可以是“账户 A–H 协调行动，以放大内容 X”。替代假设可以是“独立用户因某一外部事件而分享同一模板”。另一个假设可以是“平台因推荐排序而呈现出表面模式”。每个假设都需要一项可能削弱它的检验：早期来源、文本变化、先前顺序、事件之外的行为，以及与其他群体的比较。

参照基准应在计算前确定。它可以是同一主题的另一场讨论、同一批账户的另一时段，或一组可比用户。不能因为某个阈值能产生期望结果就选择它。如果没有适当的参照基准，应说明异常仅为描述性发现，不得赋予虚构的概率。

> **检验原则**
> 良好的研究不只是寻找更多协调行为的线索，还要寻找能够证明初始解释并非必要的数据。

第2章 现场保全

2.1 可能消失的对象

应保存帖子、个人资料、简介、图片、回复、引用、转发、链接、指标、日期和可见变更。为每个对象分配标识符，并关联其 URL、账户、平台、日期和获取方法。主页截图不能证明一个账户的全部帖子，也不能证明关系网络先前的状态。

如有经授权的导出功能或 API，应记录 endpoint 或函数名（不含机密）、版本、参数、筛选条件、分页、限制、时区、格式、日期和错误。收到的数据应以原生格式保存，并附数据字典（如有）。如果只能手动截取，应记录操作人、所用角色权限以及检查范围。不得为补齐数据集而规避访问限制。

2.2 关系与顺序

关系应作为独立对象记录：账户 A 回复 B、引用 C、分享链接 D 或关注 E。应保存证明各条关系边的内容及可见日期。没有这些参照信息的关系图可能美观，却无法核实。关系方向很重要：关注不等于被关注，引用不等于撰写了原文。

时间线应保留原始日期文字、时区、精度和含义：创建、编辑、发布、截取和指标记录是不同事件。平台可能按相关性而非时间排序。应尽可能利用帖子标识符和外部来源构建顺序，不能假定屏幕上的顺序就是实际顺序。

对象	最低记录要求	局限
帖子	URL、ID、账户、文本、多媒体和日期。	不能提供账户的完整上下文。
个人资料	URL、显示名称、简介和变更。	不能据此确定真实账户归属或自动定位。
关系	来源、类型、去向和证据。	不能表明控制方向或意图。
指标	数值、日期、含义和平台。	不能据此确定独立读者数或全部损害。
导出	参数、覆盖范围、筛选条件和数据字典。	查询范围之外不保证完整性。
截图	操作人、角色、日期和查看路径。	不能替代可用的原生格式。

2.3 隐私与比例原则

调查个人资料可能会暴露与损害无关的人。收集范围应限于必要信息，并将工作版本与公开版本分开。不得为了“证明”假设而公开个人数据。不得通过冒充身份或虚假账户访问私密个人资料；应请求授权途径，或说明这一限制。

> **安全原则**
>
> 不要让媒体损害调查造成另一项损害。报告可以证明关系，而无须公开住址、电话、未成年人信息、照片或未经证实的推测身份。



图1. 应在网络消失前完成保全。对象、关系、时间和覆盖范围。编辑重构；不构成真实证据。

第3章 内容与时间线

3.1 文本、变体与早期来源

应比较原文及其变体：词语、话题标签、共同错误、空格、链接、表情符号、格式和截选片段。公开模板可以解释相似之处；罕见错误可能暗示共同来源，但不能识别作者。应寻找早期版本，并记录是否可能存在超出调查范围的更早版本。

图片和视频可能共用文件、标记、裁剪或元数据。如果同一文件是热门图片或由某组织提供，两个账户使用该文件并不能证明协调行为。应分析集合内谁最先发布、文件如何变化，以及账户是否使用相关的链接参数或名称。场景真实性应通过另一种方法评估。

3.2 时间窗口与频率

同时性必须有单位和参照基准。“同时”是指同一秒、同一分钟、同一小时还是同一天？突发新闻可能产生数千条发布时间接近的帖子。应结合时区和精度，将分布与此前时段及其他讨论进行比较。不得在看到某个时间窗口恰好将可疑账户归为一组后才选择它。

发布频率可能暗示自动化或团队协作，也可能源于定时开展的活动或非常活跃的个人。应结合背景分析停顿、规律性、内容多样性和发布时间。连续24小时发布的账户并不自动就是机器人：它可能由不同时区的多名管理员运营。

3.3 链接与参数

应从域名、路径、重定向、参数、活动、注册日期（如公开）以及与其他对象的关系等方面分析链接。相同参数可能表明复制了同一链接、使用模板或共享配置，但不能证明共同所有权。应保存重定向序列和最终内容，同时避免在生产环境访问危险目标。

线索	正当的替代解释	核实方法
相同的文本错误	共用模板或引用内容。	早期来源及账户间的变化。
发布时间接近	突发新闻或预定活动。	参照分布和先前行为。
相同链接	热门来源或公开活动。	参数、首次使用和重定向。
相同图片	传播素材或热门趋势。	文件、版本、裁剪和首次发布。
持续活动	轮班、定时发布或高强度使用。	操作类型、时区和可用记录。

虚构案例

八个账户在两分钟内发布同一链接。参照基准显示，数千人因一则新闻而分享该链接。然而，只有这八个账户使用相同的罕见参数和相同的文本错误，而且此前就曾共同行动。协调行为的判断因多项线索相互印证而增强，而不是因为这两分钟。

第4章 协调行为与假设

4.1 相互印证的指标

应构建矩阵，纳入内容、时间、链接、历史记录、关系、个人资料变更、先前行为和可能的外部来源。每项指标都应有替代解释和核实方法。不能通过对信号简单投票来判断其证明力：一些信号彼此依赖，另一些则可能在平台上很常见。

参照基准可用于判断某一频率或关系是否异常。可以将间隔分布与此前时段比较，或在保留相关特征的前提下，与受控的数据置换结果比较。如果使用模拟，应记录种子、规则、假设和迭代次数。如果模型不能代表实际过程，就不得给出统计概率。

4.2 账户年龄、变更与社群

平台迁移或邀请活动可能导致大量新账户出现。应将创建日期作为一组数据进行分析，并与前后的活动比较。同时更改名称、图片或简介可能暗示使用模板，也可能源于社群活动。应在可见历史记录消失前将其保存。

账户相互关注可能表明存在网络，也可能只是志趣相投的社群。应与其他群体比较连接密度、互关情况、群体外活动和先前关系。密度不能证明集中控制。小群体可能因为成员彼此认识而高度互联；关系图必须辅以内容和时间线。

4.3 自动化评估

自动化判断应以技术行为为依据：按一定间隔重复操作、使用特定接口、内容模式、即时响应，以及与合理人类活动不相符的持续性。即便如此，也存在合法的定时发布工具和按例行流程工作的人工团队。如果没有记录，报告可以写“行为与自动化相符”，但不能断言使用了某一具体工具。

维度	问题	推断边界
内容	存在变体，还是只有逐字复制的副本？	模板不等于集中控制。
时间	与参照基准相比，该模式是否异常？	同时性不等于机器人。

维度	问题	推断边界
历史记录	协调行为是否早于该事件?	新账户可能源于平台迁移。
关系	密度是否高于可比社群?	友谊和共同兴趣也会形成密集关系图。
接口	是否有自动化证据?	存在合法的定时发布。
归因	哪种来源能识别实际控制者?	仅凭 IP 或图片并不足够。

有依据的结论

“该组账户在内容、参数、顺序和先前行为上的相似性与协调行为相符。现有覆盖范围不能支持对某个人或具体工具的归因。”



图2. 协调行为应通过检验替代解释来验证。依据是相互印证的指标，而非单一醒目的信号。编辑重构；不构成真实证据。

第5章 关系图与基础设施

5.1 节点不等于个人

根据图例，节点可以代表账户、帖子、链接或基础设施。边代表有记录的关系，而不是命令。关系图应包括类型、方向、时段、来源和覆盖范围。如果使用算法对节点分组，应记录方法和参数；未经定性验证，不得将聚类呈现为真实组织。

处于中心位置的账户可能只是热门来源。连接不同群体的桥梁可能是媒体，也可能是回应所有人的个人。中心性指标用于引导检查，不能证明控制关系。报告应保存关系边列表，以便他人核实两个节点为何相连。

5.2 域名、IP 与共享服务

一个 IP 地址可能属于平台、VPN、企业、合住家庭或动态分配服务。一个域名可能与数千个网站共用托管、DNS 或证书。共享基础设施可以引导信息请求和分析，但不能证明账户具有共同所有权。应避免据此对个人进行地理定位。

必要的技术记录应通过合法渠道请求。不得进行侵入式扫描，也不得查询泄露的凭据数据库来关联账户。如果来源公开，应记录日期和覆盖范围。数据泄露并不意味着获得下载、合并或公开个人数据的授权。

5.3 归因分级

级别	可以作出的论断	不能由此推导的结论
内容	这些帖子及版本曾经存在。	所叙述的事件确实发生。
行为	这些操作呈现一种模式。	该账户是机器人。
关系	账户之间以这种方式互动。	账户之间相互控制。
基础设施	共用服务或参数。	同一所有者或位置。
协调行为	多项相互印证的线索与协调行为相符。	由某个人统一指挥。
账户归属	由合法来源和上下文证实的控制关系。	不得根据姓名、照片或 IP 推断。

> **专业边界**
>
> 报告可以对协调行为作出明确结论，同时对作者身份保持审慎。要证明网络的行为方式，并不需要确定其背后是谁。

第6章 媒体损害与报告

6.1 范围与后果

应区分内容、行为、可见传播范围和经证实的后果。展示次数不等于独立读者数，表情回应不等于支持，评论也不能证明观点改变。报告应记录指标及其日期和已知含义，不得将其转化为通用的损害数值。

损害应通过通信记录、用工决定、合同、证言、报告、对受影响者的援助及其他来源予以记录。不能不分析其他原因，就把活动结束后发生的一切都归因于该活动。证据保存可以证明某种模式曾经存在；因果关系还需要时间顺序和补充证据。

6.2 可复现的技术报告

报告包括委托事项、范围、来源、方法、数据字典、时间线、指标、参照基准、关系图、替代解释、发现、局限和附录。应公开对象标识符和查询条件，以便重复分析。有关行为的论断应关联到帖子，有关影响的论断应关联到具体文件。

公开版本可以省略理解方法所不需要的账户或数据，但不得隐藏推理过程。如果删除某个帖子后一项论断就发生变化，应复核其稳健性。如果无法访问私密内容或平台记录，应说明覆盖范围，不得以推测补齐。

6.3 后续行动

向平台举报时，应指明内容、账户、模式和证据，不得以公开指控代替。撤下或保存证据的请求应记录日期和受理编号。与受影响者沟通时，应避免重复有害内容，并说明正在采取的措施。如存在威胁或人身风险，应优先联系当地紧急渠道。

《数字服务法》规范中介服务以及某些超大型平台的系统性风险。欧盟条例 (UE) 2024/900 涉及政治广告服务的透明度和定向投放，并对自发内容设有边界。这些法规不会自动适用于所有账户或国家，也不会把虚假信息变成普遍适用的违法类别。[1][2]

> **结语**
>
> 报告的目的，是说明一种行为及其边界，而不是在缺乏证据的情况下提出新的指控。证据应通过适当渠道提交，而不是用于公开羞辱。

[1] Reglamento (UE) 2022/2065《数字服务法》。中介服务制度、某些超大型平台和搜索引擎的系统性风险管理，以及内容规则。该条例不会把所有模式都变成协调行为的证据，也不会把所有观点都变成非法内容。 官方在线来源

[2] Reglamento (UE) 2024/900，关于政治广告透明度和定向投放。针对政治广告服务及相关风险的具体规则；并非不加区分地适用于用户的所有自发内容。 官方在线来源



图3. 报告区分模式、基础设施和个人。结论不得超出来源的证明力。编辑重构；不构成真实证据。

附录A 分析格式

A.1 账户与内容清单

字段	必要记录	核查要求
账户 / URL	标识符、平台、个人资料和观察日期。	不得填写推测的个人姓名。
帖子	ID、文本、版本、多媒体和原始日期文字。	对象已保存。
关系	来源、类型、去向和证据。	不得推断控制关系。
时间	时区、精度和含义。	不要混淆创建时间与截取时间。
指标	数值、日期和平台定义的含义。	不能据此确定独立读者数。
覆盖范围	查询、筛选条件、访问权限和缺失项。	不得断言具有完整性。
隐私	敏感数据、限制和公开版本。	真正落实最小化。

A.2 指标矩阵

线索	替代解释	核实方法	有限结论
文本 / 共同错误	模板或引用。	早期来源和变体。	[ ]
接近的时间窗口	新闻或事件。	参照基准和此前分布。	[ ]

线索	替代解释	核实方法	有限结论
链接参数	复制链接或公开活动。	首次使用和重定向。	[]
账户年龄相近	平台迁移或活动。	先前活动和背景。	[]
密集关系图	志趣相投的社群。	参照基准和群体外行为。	[]
共同基础设施	共用服务提供商。	注册记录和其他账户。	[]

A.3 报告结构

操作性目录

1. 委托事项、问题、范围和排除标准
2. 来源、覆盖范围、数据字典和局限
3. 证据保存与对象清单
4. 时间线与内容变体
5. 协调行为指标与参照基准
6. 关系与具有可核实边的关系图
7. 替代假设与阴性结果
8. 可见传播范围与经证实的后果
9. 按归因级别列出结论
10. 隐私、交付、附录和版本
11. 已查阅的法律与技术来源

A.4 使用模拟时的记录

最低记录要求

问题与指标：[比较内容]
纳入的数据与覆盖范围：[来源和筛选条件]
所选参照基准及理由：[时段或群体]
置换规则：[保留什么、改变什么]
种子与工具版本：[用于重复实验]
迭代次数：[数量与理由]
结果：[分布与观察结果]
未涵盖的假设：[局限]
可作出的结论：[不得使用虚构概率]

附录B 法律框架与最终检查

帖子和记录的证据涉及电子文件的认可、保存与评价。墨西哥根据过渡安排适用 CCom 89–94 和1205以及 CFPC/CNPCF；秘鲁区分签名与程序；智利区分签名和日期；阿根廷重视可靠性；哥伦比亚和厄瓜多

尔要求连同来源和日期一并保存；西班牙结合适用 eIDAS、LEC 和数字服务规则。未经审查适用制度，不得将自发内容等同于广告。[3][4][5][6][7][8][9][10][11][12][13][14]

网络调查也涉及个人数据。应遵循目的限制、比例原则、安全性和最小化原则；不得毫无依据地合并来源以识别个人。言论自由和内容分析应与协调行为评估分开。即使账户使用化名，指控其为“机器人”也可能是错误且有害的。[15][16][17][18]

最终检查	验收问题
覆盖范围	查询、筛选条件、时段和缺失项是否均已记录？
对象	每条帖子、每项关系和每个指标是否都有来源？
协调行为	是否有多项指标相互印证并进行了比较，而不只是巧合？
替代解释	是否评估了模板、事件、社群和平台因素？
关系图	是否明确节点不等于个人、关系边不等于控制？
归因	结论是否没有虚构账户归属者或工具？
损害	传播范围与后果是否分开记录并经证实？
隐私	调查是否避免了不必要的暴露？

[3]墨西哥《商法典》，第89–94条和第1205条：数据电文的中立性、归属、书面形式、原件、完整性、可访问性和采信。官方汇编版本。官方在线来源

[4]《国家民事和家庭程序法典》，第348–350条。含15-01-2026改革的汇编版本。其适用是渐进的，并取决于相关宣告。 官方在线来源

[5]秘鲁。IOFE 条例，DS 052-2008-PCM，第3条和第4条：对经数字签名的电子文件的要求与采信。 官方在线来源

[6]秘鲁。《民事诉讼法典》，第188–197条和第245.5条：目的、合法性、证据手段、举证责任、评价以及通过技术手段确定日期。 官方在线来源

[7]智利。Ley 19.799（关于电子文件和电子签名），第1–5条：等效性、书面形式、简单 / 高级签名、日期和证明力。 官方在线来源

[8]阿根廷。《民法与商法典》，第318–319条：以任何媒介进行的书信往来，以及对载体和技术程序可靠性的权衡。 官方在线来源

[9]哥伦比亚。Ley 527 de 1999，第5–13、16–25和28条：数据电文、书面形式、原件、完整性、可采性、保存、发送、接收和数字签名。官方在线来源

[10]厄瓜多尔。《电子商务、电子签名和数据电文法》（Ley 67），第2、6–8、10–16条：等效性、书面形式、原件、保存、来源、发送、接收和电子签名。 官方在线来源

[11]Reglamento (UE) 910/2014（eIDAS），第25–26和46条：不得因电子签名和电子文件的格式而加以歧视；高级电子签名；合格电子签名的法律效力。 官方在线来源

[12]西班牙。《民事诉讼法》，第326条和第384条：私人文件、异议、用于保存、访问或复制数据的工具、检查、保管和自由心证。 官方在线来源

[13]Reglamento (UE) 2022/2065《数字服务法》。中介服务制度、某些超大型平台和搜索引擎的系统性风险管理，以及内容规则。该条例不会把所有模式都变成协调行为的证据，也不会把所有观点都变成非法内容。 官方在线来源

[14]Reglamento (UE) 2024/900，关于政治广告透明度和定向投放。针对政治广告服务及相关风险的具体规则；并非不加区分地适用于用户的所有自发内容。 官方在线来源

[15]墨西哥。《私营主体持有个人数据联邦保护法》，文本公布于20-03-2025，改革日期为14-11-2025。第5–9、18–20和31条：原则、安全、保密、数据安全事件和权利请求处理。当前联邦主管机构为反腐败与善治部。 官方在线来源

[16]哥伦比亚。Ley Estatutaria 1581 de 2012，第4、8、12、17–18和26条：原则、权利、信息、责任人与处理人的义务，以及向第三国传输。 官方在线来源

[17]厄瓜多尔。《个人数据保护组织法》，Registro Oficial Suplemento 459 de 26-05-2021。第10、37–44条：原则、安全措施、设计即保护、风险及事件发生时的处理。 官方在线来源

[18]欧盟。Reglamento (UE) 2016/679，第5、25、28和32–34条：原则、设计即保护、处理者、安全以及安全事件的通知 / 通报。西班牙还要求审查适用的国内和行业立法。 官方在线来源

结语

网络的存在应通过对象、顺序和关系证明。不能为了补全关系图而虚构个人。