Conti勒索软件通信网络的多尺度时间结构

Cameron Cornell、Matt hew Roughan、Lewis Mitchell、Chad Whelan、David Bright 和 Callum Jones

摘要——通信网络能够通过累积的局部互动推断更广泛的组织结构。尽管网络犯罪组织行事隐秘，但它们尤其容易受到此类推断，因为分布式运作需要通过集中式数字通信基础设施进行协调。Conti勒索软件组织内部通信的公开泄露，提供了这类协调活动罕见的纵向记录。然而，分析此类纵向记录的常见方法，会将互动汇总为静态网络，或将通信过程建模为平稳过程；这两种方法都假定时间同质性，而这一假定在犯罪组织中鲜少经过检验。本文表明，在对Conti记录考察的每个尺度上，都存在显著的时间异质性；并证明其中很大一部分可以通过恰当且由诊断结果指导的事件表示方式和观测期选择加以解释。将快速消息突发合并为对话片段，可使通信时序更接近恒强度基准，并使较长时间尺度上的结构更加清晰；由此呈现出一系列不同的通信状态，其中包括协调迁移平台后发生的一次重大转变。即便如此，这些状态内部的异质性仍然存在，最明显的是边缘参与者不断更替，而高度活跃的行为主体则始终可以被观测到。总体而言，这些发现表明，在网络犯罪网络的分析、建模和纵向监测中，应明确考虑多尺度时间动态。

索引术语 rms—网络犯罪网络、网络演化、非平稳性、时间聚合、时序网络

arXiv:2611.32181v1 [physics.soc-ph] 24 Nov 2026

1 引言

通信网络广泛存在于各种技术和社会系统中，为研究通信实体之间的互动提供了自然框架[1], [2]。相关实例涵盖电信基础设施 [3], [4] 、在线社交平台[5], [6], 以及组织和协作系统[7],[8]。尽管个体通信主要用于促进局部信息交换与协调，但由大量此类互动形成的总体模式，往往能够揭示底层系统的更高层次属性。组织结构、具有影响力的参与者以及集体行为模式，可能会从大量个体互动的积累中显现出来，尽管这些特征并未被明确编码在任何单条消息中。因此，通信并非只是组织的副产品，也是组织最主要的可观测表现之一，为理解协调、层级结构和集体行为提供了窗口。

网络犯罪组织是通信系统中一个尤其值得关注的例子 [9], [10]。不同于许多传统犯罪网络——在这些网络中，关系往往必须通过逮捕记录、交易记录、共同犯罪记录或监控数据间接推断——网络犯罪活动相对集中地通过数字通信平台开展。现代勒索软件行动具有地理分散的特点，因此需要专业化行为主体之间持续进行远程协调，使得通信基础设施成为组织活动开展的主要机制，令这种通信基础设施成为组织活动开展的主要机制。尽管通信记录不一定能捕捉参与者之间的所有互动，但它们为观察互动过程提供了相对丰富的视角。因此，通信数据为我们直接通过支撑其运作的互动，考察网络犯罪组织的结构与动态，提供了宝贵机会。

研究此类通信过程的独特机会于2022年初出现，当时Conti勒索软件组织的内部通信遭到公开泄露 [11], [12], [13]。在这一时期，Conti是规模最大、活动最为活跃的勒索软件团伙之一，其活动涵盖勒索软件部署、敲诈勒索以及为网络犯罪提供支撑的服务。该团伙就俄乌冲突发表公开声明后，一名疑似内部人员将一大批内部通信档案发布到网上。由此形成的数据集包含168,740条带时间戳的消息，这些消息由450个不同的化名用户ID（下文称为参与者）在二十个月期间相互交换。这种网络规模、时间深度与直接通信记录的结合，为了解一个大型网络犯罪组织的内部运作提供了异常详尽的视角。

通信记录通常以聚合方式进行分析，从而提供底层组织拓扑的静态视图。然而，即使在常规运作期间，生成这些网络的互动也可能发生显著变化：行为主体进入或离开系统，参与程度起伏不定，互动结构也会随时间重新配置。因此，相较于单一的静态结构，观察到的通信网络或许更适合被视为一个动态重新配置的系统，这也促使人们

• *C. Cornell*、*M. Roughan* 和 *L. Mitchell* 任职于阿德莱德数据科学中心、阿德莱德大学数学科学学院，地址为澳大利亚南澳大利亚州 *5005*。

• *C. Whelan*、*D. Bright* 和 *C. Jones* 就职于澳大利亚迪肯大学人文与社会科学学院。

• 本研究由澳大利亚政府通过国家情报与安全办公室探索研究资助（*NISDRG*）项目 *[NI2301000042]*资助。

需要对组织行为进行时间分辨分析 [14], [15]。与更广泛的通信网络分析领域一样，现有对网络犯罪通信网络的分析主要基于时间聚合表示，因此难以直接观察这些不断演变的通信过程。

为弥补这一局限，我们从多个视角考察 Conti 通信网络中的时间异质性，这些视角分别对应时间活动的不同分辨率。

- **对话微观结构**。我们考察突发通信动态，并展示对话活动如何在消息级别产生显著的时间聚集现象。我们提出一种简单的突发事件合并程序，将二元组内快速往来的消息合并为对话片段，并展示这种表示方式更贴近底层交互过程，从而能够区分真实的网络动态与微观尺度对话效应。在随后的状态分析中，这一点尤为明显：突发合并使状态内的平均邻接相关性提高了约 24%。此外，将合并后的过程与不同阈值下的泊松零模型进行比较，可为选择后续分析所依据的事件时间尺度提供简单标准。

- **通信状态**。我们根据通信结构随时间的变化，识别出四种不同的通信状态。这些状态在交互模式和组织活动水平方面各不相同。将网络视为由一系列 14 天窗口构成，我们表明，识别出的状态将 0.211 的全局平均跨窗口相关性分解为状态内的 0.428 和状态间的 0.085，揭示出通信结构相对稳定的时期。我们还考察了状态转变与已观察到的行动事件之间的关系，其中有证据表明，一次重大的结构转变与一次有组织的平台迁移有关联。

- **参与动态与可观测性**。我们考察行为主体的生命周期、更替和发现情况，以评估组织参与如何随时间被观测到。高活跃度的行为主体会被迅速且持续地发现，而低活跃度的参与者在每个阶段仍会持续被发现，其发现速率无法仅由其较低的总体活动水平来解释。因此，有限的观测期可能会捕捉到主要通信者，却严重低估网络外围。

总体而言，这些分析以更高的时间分辨率呈现了网络犯罪分子的通信，凸显出有必要考虑通信结构、参与者活动和组织协调随时间发生的变化。

2 相关研究

2.1 犯罪组织网络分析

在犯罪学领域，将网络分析应用于犯罪组织由来已久，最初源于对其在犯罪情报方面应用前景的早期评估 [9], ，并逐渐发展成为大量研究成果，用于刻画犯罪团伙的结构、识别处于战略位置的行动者，并为瓦解策略提供依据 [10], [16]。这一研究文献始终关注犯罪网络数据固有的观测局限性：此类数据通常必须根据逮捕记录、监控数据或电话监听等来源进行重构，因此只能形成边界不确定且不完整的网络表征 [9], [17]。通信记录能够相对直接地进行观测，捕捉互动过程本身，而不必通过共现或关联来推断关系 [17]。然而，这类研究大多在单一时间点考察犯罪网络。少量纵向研究记录了毒品贩运网络在多年间的结构变化 [18], [19] ，并使用随机行动者导向方法对网络形成进行建模 [20],，表明犯罪网络会因应运营需求和执法压力而发生显著重组 [19], [21]。尽管如此，此类研究所能达到的时间分辨率仍然较为粗略：网络被汇总为少量跨数月或跨数年的时间波次，其划分依据是数据可得性，而非组织的内在动态。因此，在进行任何详细的数学建模之前，研究往往已经作出了统计平稳性的假设。

网络犯罪的发展使这一研究计划扩展到在线犯罪网络，在这些网络中，数字轨迹数据提供了丰富得多的观测信息。网络分析方法已被应用于黑客社群 [22],暗网市场 [23], 和网站篡改生态系统[24], ，而组织研究则将逐利型网络犯罪团伙描述为日益呈现企业特征的组织，其内部表现出劳动分工 [25]。然而，即使有纵向数字记录可供使用，相关分析通常仍是通过比较离散的网络快照来进行，而不是对作为基础的交互流进行时间分辨处理 [24]。

2.2 ContiLeak 分析

2022年，Conti 内部通信内容遭到泄露，由此催生了一批虽规模不大但不断增长的研究，探讨大型勒索软件企业的内部运作。现有研究利用泄露语料库追踪赎金支付并描述该组织的商业模式 [11],，考察洗钱策略 [28], ，通过机器学习识别讨论主题 [29], ，并结合网络与内容分析绘制该组织的组织结构图 [12], [13]。后者揭示了一个层级分明、类似商业企业的组织，其领导职能明确、任务专业化程度高，与合法企业中观察到的结构如出一辙 [12]。

这些研究确立了 Conti 语料库作为网络犯罪组织独一无二的详尽观察记录。

表 1：Conti 研究及其对时间结构处理方式的比较。

研究	重点	时间方面的考量
早期 Conti 研究 [11], [12], [13]	刻画 Conti 的运作，层级结构和组织角色。	主要采用聚合网络与内容分析，并结合在 [12] 中进行对话预处理。
Manatova 等人。（2026） [26]	分析组织结构与韧性。	将消息分组为对话，以构建加权的聚合无向网络，并通过人工评估对分段进行评估。评估。
Sadewo 等人（2026） [27]	解释管理沟通的变化并使用关系事件模型进行分析。	合并间隔不到一分钟的消息片段，并进行比较针对所选时长大致相等的时期，分析管理效应模型稳定性。
本研究	系统刻画时间异质性及其对网络的影响分析。	评估对话聚合如何改变到达间隔统计及后续分析；识别通信状态并将状态转变与组织事件联系起来；考察剩余的时间异质性，通过在状态中发现参与者。

然而，早期分析主要基于时间聚合表示，往往将长达二十个月的完整通信记录投射到单一静态结构上。更广泛的犯罪网络文献表明，此类组织会随时间发生显著重组 [18], [19],，因此，聚合表示可能会将不同的组织阶段混为一谈，纳入同一份概述。近期研究日益纳入时间因素 [26], [27], ，通常用于支撑应用型组织分析，这凸显了系统考察这些数据中时间异质性影响的必要性。本研究系统地考察了这些选择：对话聚合如何改变观测到的时间统计特征，如何识别相对稳定的通信状态，以及这些状态中还存在哪些时间异质性。表 1 总结了这些研究的侧重点及其对时间因素的考量。

2.3 时序网络与人类通信动态

除了犯罪学之外，围绕时序网络也已发展出大量方法学文献。在时序网络中，交互发生的时间被保留为表征中的显式要素，而不是通过聚合将其消去 [14], [15]。这类文献的一项核心发现是，时间聚合方式的选择会产生重要影响：聚合网络的结构属性会系统性地取决于聚合窗口的长度和位置 [30], [31], ，而且通常不存在单一、天然适用的聚合时间尺度，因为相关动态会出现在多个时间分辨率上 [14], [30]。相关研究还进一步表明，有限观测窗口会系统性地扭曲估计得到的交互统计量，包括事件间时间分布 [32]。这些考量直接促使本研究采用多分辨率方法，将对话微观结构、制度层面的重组和参与动态视为发生于不同时间尺度上的不同现象。

在最短时间尺度上，人类通信已被证实在时间分布上并不均匀。间隔-

人类活动中的事件时间分布呈现重尾，与无记忆恒定速率行为不符。这一现象被归因于多种因素，例如任务执行中的优先级排队机制 [33] ，以及周期性活动周期与相关活动级联的叠加 [34]。 [34], 提出的级联过程视角与本研究尤为相关：在这一视角下，非齐次泊松过程支配活跃区间的启动，而多个事件会在这些区间内快速连续发生。第 5 节提出的突发事件合并程序以非参数方式落实了与之密切相关的双时间尺度视角，将快速连续的消息视为对话回合；这些回合的启动，而非其内部回复结构，才是具有组织意义的事件。若需要参数化的时间结构，自激点过程模型便是自然的形式化对应方法 [35], [36], ，但本文不对这类模型展开探讨。

用于评估这些动态的一种自然零模型是二元泊松模型，其中为每个二元组指定固定的基线交互强度，并假设事件以恒定速率独立发生。该模型提供了一个恒定速率基准，其偏离情况可用于识别对话和组织层面上所关注的时序结构。第6节所考察的通信状态边界识别，与网络中的变点检测这一更广泛的研究领域相关，该领域已有不断发展的方法学文献 [37], ；第7节的参与者发现分析则借鉴了源自生态学的物种丰富度估计技术 [38], [39], [40]，并将其应用于犯罪学中的隐匿人口估计 [41]。

3 数据

该数据集包含 Conti 网络犯罪组织在2020年6月21日至2022年3月2日期间的内部通信泄露语料库，由 Northwave Security 公开提供，内容为译成英文的 Jabber 聊天 CSV 文件 [42]。其中包含450个不同的化名用户ID之间168,740条带时间戳的定向消息。对于每条消息，数据集均记录了源标识符、目标标识符，以及经过编码和部分解码的消息内容。

数据集还记录了时间戳。我们将每个用户ID视为一个网络节点，并在全文中将这些ID称为参与者，不过同一个人可能使用多个ID。

通信通过基于 Jabber/XMPP 的内部消息基础设施进行，这类基础设施因支持私有、自托管服务器而常用于网络犯罪活动。消息以从该系统提取的日志形式存储，时间戳通常精确到分钟以内。普遍认为，此次泄露源于该团体内部的分歧，导致聊天记录及相关运营数据被公开发布。迪肯大学人类研究伦理委员会（高于低风险级别）批准使用这些公开发布的 Conti 数据（批准编号 2023-165），理由是无法实际取得 Conti 聊天记录泄露事件相关成员的知情同意，且项目带来的益处超过任何潜在风险。分析使用化名用户ID，且未尝试识别任何个人。现有数据的一个局限是，2020年11月16日至2021年1月29日期间存在一段中断期，没有可用的通信记录。

令 V 表示参与者集合，并令

$$E = \{(i, j, t)\},$$

对于 $i, j \in V$，将带时间戳的有向通信事件集合记为，其中每个元素对应于在时间t由行为主体 i 发送给行为主体 j 的一条观测消息。时间戳经过重新索引，使得 $t = 0$ 对应于观测期的开始，并以天数为单位表示。

因此，可将该通信系统视为一个时间有向多重图，其中任意有序参与者对之间都允许存在多条带时间戳的边。有序参与者对 （i， j）定义了有向二元组，这些二元组构成后续时间分析和交互层面分析的基础。

4 聚合网络结构

我们首先考察通信系统的非时间投影，将指定观测窗口内的带时间戳消息事件进行聚合。由此得到有向网络表示，其中边权重对应于该窗口内参与者之间发送的消息总数。

形式化地，对于任意时间窗口 $[t_0, t_1]$，定义加权邻接矩阵 $W^{[t_0,t_1]}$ 为

$$W_{ij}^{[t_0,t_1]} = \sum_{(i,j,t)\in E} \mathbb{1}(t_0 \le t \le t_1),$$

使得 $W_{ij}^{[t_0,t_1]}$ 记录时间区间内从行为主体 i发送给行为主体 j 的消息总数。

我们还定义了相应的二元邻接矩阵

$$A_{ij}^{[t_0,t_1]} = \mathbb{1}\big(W_{ij}^{[t_0,t_1]} > 0\big),$$

该网络仅记录是否发生通信，而不考虑消息数量。

除非另有说明，未加索引的矩阵 W 和A 表示对整个观测期进行聚合。所得聚合网络的汇总统计量见表2。

表2：汇总通信网络的汇总统计量。

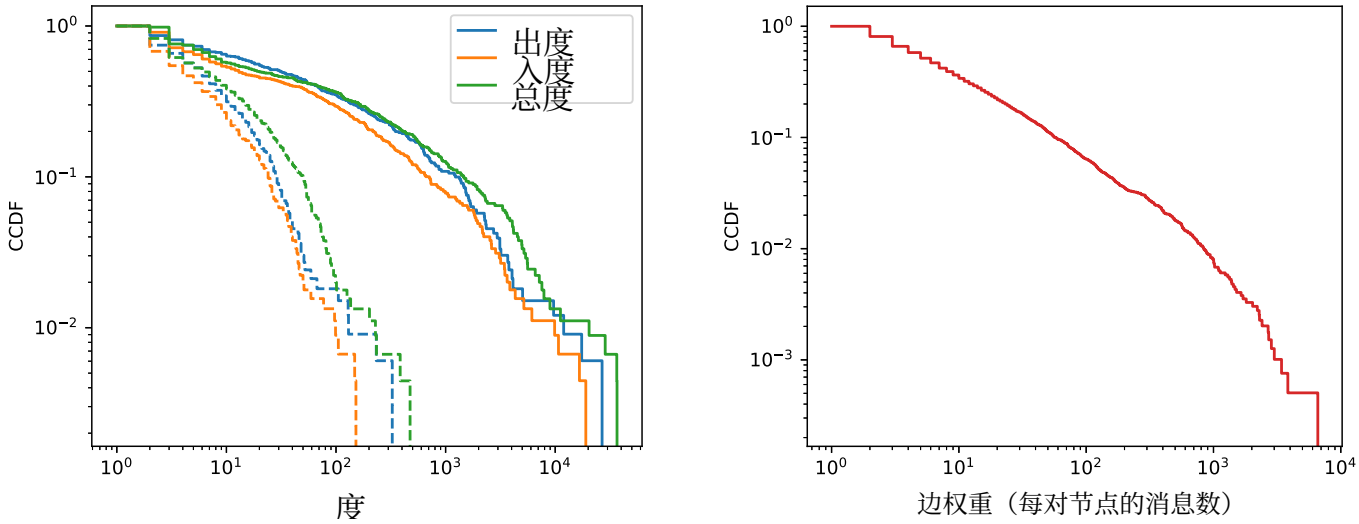
统计量	值
节点数 $\lvert V\rvert$	450
消息数 $\lvert E\rvert$	168,740
每个节点的消息数 $\lvert E\rvert/\lvert V\rvert$	375
平均度	8.8
出度中位数	2
入度中位数	3
活跃二元组 ($W_{ij} > 0$)	1.96%
互惠性	62.3%

表2总结了汇总后的通信网络。我们将度定义为二元度数，其中出度和入度分别对应与每个行为主体相关联的不同接收者和发送者的数量，不考虑消息量。在此背景下，度反映了观察到的行为主体至少通信过一次的独立个体数量。由此形成的网络稀疏且分布偏斜，450个节点的平均度为8.8，出度和入度的中位数分别为2和3，这表明大多数行为主体仅与网络中的一小部分成员互动。整体情况也体现了这一点：仅有1.96%的潜在二元组处于活跃状态。

互惠性定义为表现出双向通信的活跃二元组所占比例，即在至少一个方向处于活跃状态的条件下， $W_{ij} > 0$ 和 $W_{ji} > 0$两个方向均活跃的配对比例。观测到的互惠性为62.3%，表明大多数活跃连接都是双向的。这与该网络用于协调通信的情况相符；若仅考虑观测到的消息数超过一条的配对，互惠性则升至 72%，若仅考虑消息数超过五条的配对，则升至 89%，这表明非互惠交互集中在低频交换中。

图1a展示了通信网络中二元（虚线）和加权（实线）出度、入度及总度的互补累积分布函数。加权度分布呈现出明显的重尾行为，概率缓慢衰减，不过相较于纯幂律预期的线性形式，其曲线存在显著弯曲。相应的二元度分布总体形式相似，但分布范围要小得多。在这两种表示中，出度、入度和总度在整个范围内都高度重合，彼此差异极小，这与网络中观察到的消息交互大多具有互惠性的特点相符。

相比之下，图1b所示的边权重互补累积分布函数（CCDF）在双对数尺度下，其支撑集的相当大一部分范围内呈现近似线性趋势，与幂律行为一致。这一趋势在上尾部截断，可能反映了由人类驱动的网络中持续通信频率的实际限制。该分布的汇总统计量显示出显著的异质性：每个活跃二元组平均有42条消息，中位数为5条，最大值为6601条，这与分布高度偏斜的特征一致



（a）加权（实线）和二元（虚线）节点的互补累积分布函数度（出度、入度和总度）。

（b）边权重（每对节点的消息数）的互补累积分布函数。

图 1：节点度和边权重在双对数尺度上的互补累积分布函数。

互动结构。

4.1 泊松零模型

聚合网络记录了与每个二元组相关的总通信活动，但未描述这些活动如何随时间分布。为单独考察通信的时间结构，不受交互频率差异的影响，我们引入泊松到达零模型。

在该模型下，每一对有序参与者 i、j 之间的通信均被视为相互独立的齐次泊松过程，其速率参数因二元组而异，为 λ_{ij}。因此，对于完全观测的时间区间 $[t_0, t_1]$，相应的消息计数满足

$$W_{ij}^{[t_0,t_1]} \sim \mathrm{Poisson}\big(\lambda_{ij}(t_1 - t_0)\big). \tag{1}$$

不同二元组之间以及不重叠区间之间的计数彼此独立。因此，网络中的通信频率可能存在显著差异，但在每个二元组内，通信频率随时间保持不变。

令 T 表示可获得通信记录的总时长，不包括第 3 节所述的不连续时段。根据聚合消息计数估计二元组特定的速率如下：

$$\hat{\lambda}_{ij} = \frac{W_{ij}}{T}. \tag{2}$$

因此，拟合模型在期望意义上重现了观测到的聚合边权重，同时消除了时间聚类、互动强度变化以及参与者活动的系统性变化。

尽管明显过于简单，但该模型为后续分析提供了一个共同基线。在较短时间尺度上，它意味着到达间隔时间服从指数分布。在较长时间尺度上，持续时间相同的观测窗口具有相同的邻接结构分布。在给定聚合二元组计数的条件下，它还提供了通过对观测到的通信事件进行随机排序而获得的参与者发现基线。

5 对话微观结构

5.1 突发通信

为研究短时间尺度上的通信动态，我们将观测到的二元组消息时间与第 4.1 节介绍的泊松到达零模型进行比较。在该模型下，消息以恒定的二元组特定速率彼此独立地发生，这意味着通信具有无记忆性，除平均互动频率之外不存在突发性或短期依赖。因此，将观测到的到达间隔时间与这一基线进行比较，可以将时间聚类与不同二元组平均通信活动的差异区分开来。

为将观察到的通信与该零模型进行比较，我们考察每个活跃二元组内连续消息之间的到达间隔时间。对于每个有序二元组 (i, j)，令

$$T_{ij} = (t_1, \ldots, t_{n_{ij}})$$

表示与该二元组相关的 n_{ij} 消息时间戳有序序列。随后，我们将相应的到达间隔序列定义为连续时间戳之差：

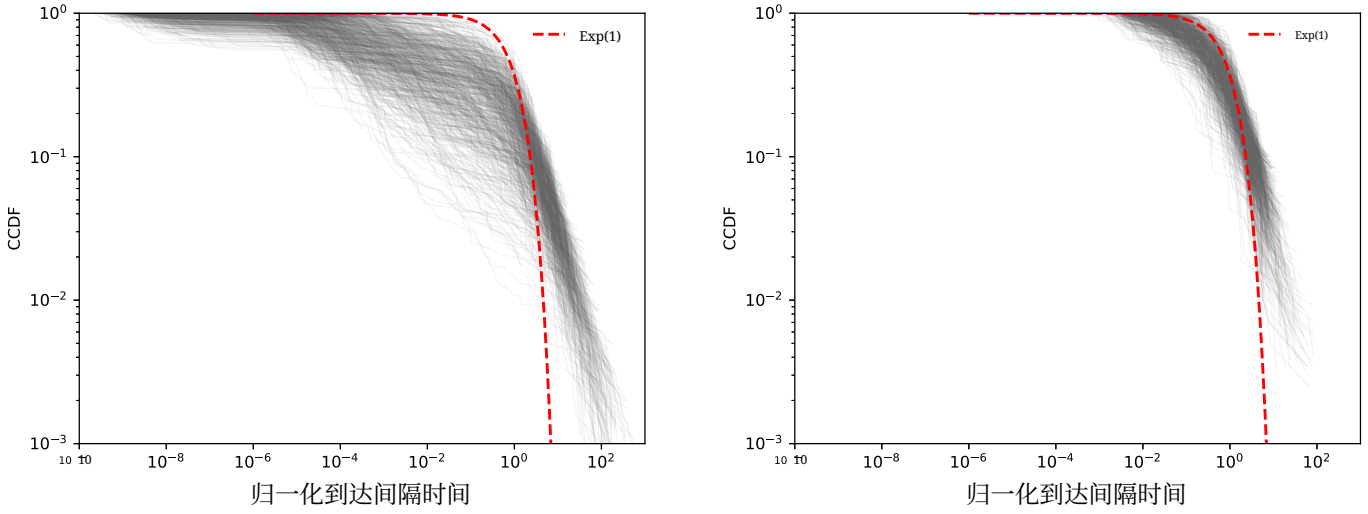
$$\tau_{ij,k} = t_{k+1} - t_k, \qquad k = 1, \ldots, n_{ij} - 1.$$

在泊松零模型下，这些到达间隔时间服从指数分布，其二元组特定的速率参数为 λ_{ij}，

$$\tau_{ij,k} \sim \mathrm{Exp}(\lambda_{ij}).$$

由于不同二元组之间的通信频率差异很大，直接比较原始到达间隔时间并无意义。为将分布形态与基线活动水平分离，我们将每个二元组内的事件间隔除以其经验均值进行归一化，

$$\tilde{\tau}_{ij,k} = \frac{\tau_{ij,k}}{\bar{\tau}_{ij}}. \tag{3}$$



(a) 原始消息。 (b) 一小时会话片段。

图 2：一小时突发折叠前后的二元组到达间隔互补累积分布函数。事件间隔按各有向二元组内的均值进行归一化。灰色曲线表示两个面板中相同的 672 个二元组；红色虚线表示 Exp(1) 指数参考分布。每个纳入的二元组在折叠后至少有 10 个事件间隔。

这样便将每个二元组的到达间隔时间重新缩放为经验均值为 1。对于齐次泊松过程，按真实速率进行缩放可得

$$\lambda_{ij}\tau_{ij,k} = \frac{\tau_{ij,k}}{E[\tau_{ij,k}]} \sim \mathrm{Exp}(1). \tag{4}$$

因此，$\mathrm{Exp}(1)$ 分布为比较通信频率各异的二元组提供了一个通用参考。由于均值是根据用于比较的同一组事件间隔估算的，经验归一化只能近似这一参考；对于观测数量较少的二元组，有限样本效应会更加显著。

图 2a 展示了根据公式 3 定义的归一化到达间隔时间在各二元组上的经验互补累积分布函数，以及泊松零模型所隐含的指数参考分布。相较于这一基准，观测到的到达间隔分布在较短间隔处的概率质量显著更大，且尾部衰减明显更慢，这表明与齐次泊松基线相比，快速连续发送消息和长时间不活跃的情况都更多。

5.2 突发合并

对于时间聚集事件序列，已有各种各样的参数模型，包括能够直接捕捉突发通信动态的自激发模型和非齐次过程模型 [35], [36] 。然而，在转向这些复杂的时间模型之前，我们首先考虑一个更简单、更直观的假设：单条消息可能并不是恰当的通信原子单位。

具体而言，我们提出，人类通信通过两种截然不同的时间机制运作：快速的对话内动态，以及较慢的对话间发起动态。在这一观点下，短时间内连续交换的多条消息可能构成同一个对话事件的一部分。这在即时消息和电子邮件系统中十分常见：一次交互事件可能包含快速连续交换的多条消息，随后经历一段较长时间的停滞。在此类情境下，原始消息事件所呈现的聚集性可能反映了这些不同时间过程的叠加，而非一个表现出复杂时间依赖的单一过程。

具体而言，我们评估这样一个问题：与原始消息相比，对话片段是否更适合用第4.1小节介绍的恒定强度泊松模型进行近似。为此，我们引入突发事件合并程序。对于每个有序二元组 (i, j)及其消息时间$T_{ij} = (t_1, \ldots, t_{n_{ij}})$，只要连续消息之间的到达间隔时间 $\tau_{ij,k}$ 不超过阈值 δ，就将其归入同一个对话事件，并将每个事件表示为其首条消息发生时刻的单个通信事件。由于对话事件是针对每个方向分别定义的，因此，两个行为主体之间快速的来回交流会在每个方向各形成一个对话事件。这种处理将对话内部快速的往来交流视为局部对话微观结构，并将其压缩为具有代表性的交互事件，从而略去与所关注的网络层面的通信结构无关的精细回复动态。

图3展示了箱线图，用于评估在逐步扩大的1分钟、1小时、1天和1周压缩窗口下，突发事件合并程序的影响。具体而言，我们报告了二元组层面的Kolmogorov–Smirnov（KS）统计量，用于衡量分布相对于$\mathrm{Exp}(1)$ 基准的偏离程度，以及每个二元组保留的事件间隔数量。我们绘制了原始数据中至少包含10个事件间隔、且在相应压缩级别下至少包含3个事件间隔的二元组，因为更少的观测值不足以提供评估分布形态所需的信息。

KS统计量在前三个压缩级别中逐步下降，表明事件间隔分布

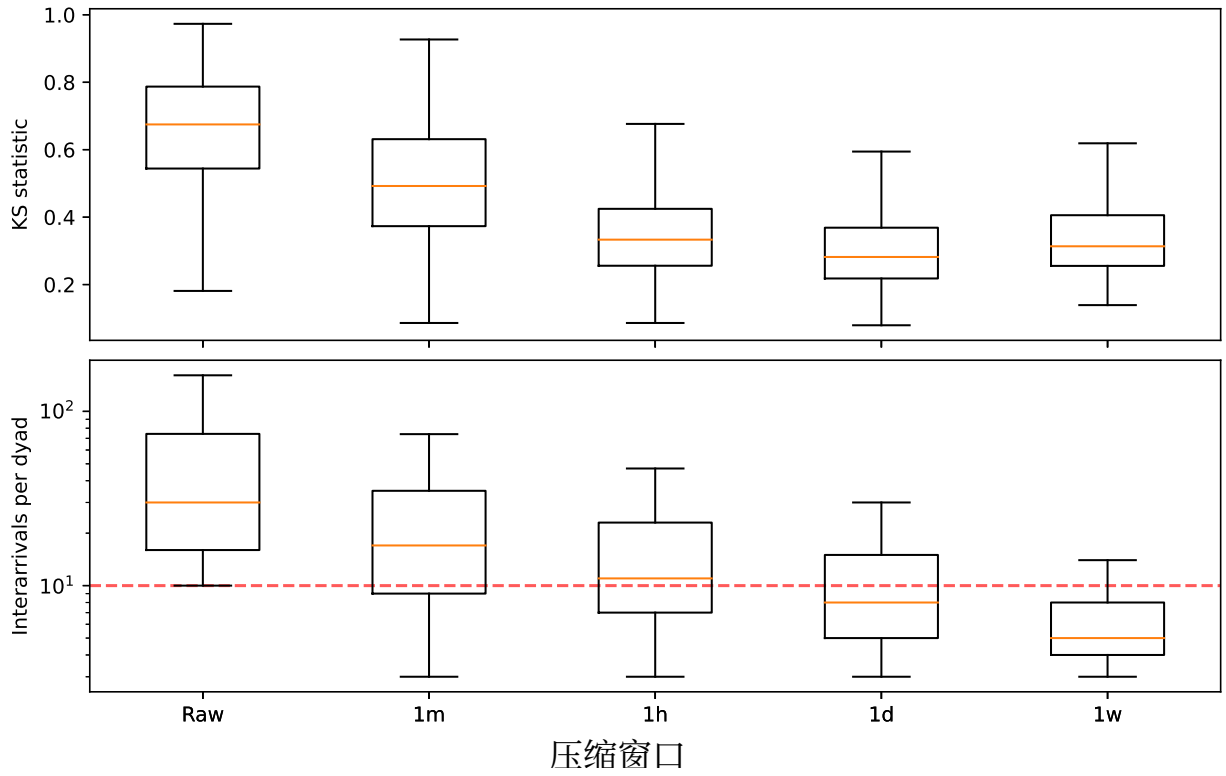


图 3：在不断增加的压缩阈值下，各二元组相对于 Exp(1) 的 KS统计量及事件间隔（对数刻度）（原始→ 1m → 1h → 1d → 1 w）。红色虚线表示每个二元组 10 个事件间隔的参考值。

越来越接近指数基准。最大的降幅出现在最初两个压缩阶段（原始→ 1分钟和1分钟 → 1小时），这表明观测到的大部分聚集性都可归因于极短时间尺度的对话交流。不过，超过1小时至1天的范围后，进一步压缩对拟合度的改善逐渐减弱，同时每个二元组保留的事件间隔数量仍在减少。尽管中位数KS统计量从1小时到1天略有下降，但在压缩至1周时又小幅回升。考虑到保留观测值相应减少，这种变化可能部分反映了有限样本效应。

总体而言，突发合并显著减少了表观的非泊松行为，但越来越激进的压缩也会带来相应的数据成本，从而减少可用于二元间隔时间分析的有效样本量。偏差的最大幅度下降发生在最初几个压缩阶段；继续压缩虽然仍会减少可用观测数量，但带来的改进逐渐递减。指数参考分布距离的缩小程度与保留观测数量之间的这种权衡，为选择合并阈值提供了一个简单的、数据驱动的标准：即进一步压缩对拟合效果几乎不再带来额外改进的临界点。对于 Conti 网络而言，这一临界点约为 1 小时；除非另有说明，后续分析均使用在此阈值下获得的对话片段作为通信事件。

在选定的一小时阈值下，图 2b 展示了由此得到的二元组事件间隔分布，并将其与图 2a 中的原始消息分布并列呈现。短归一化间隔时间的过量现象明显减少，而缓慢的尾部衰减也不再那么显著。因此，这些折叠曲线更接近泊松零模型所预测的 Exp(1) 事件间隔分布，但仍存在明显偏离。

6 通信状态

6.1 机制识别

前文所考虑的聚合网络表示，是通过将带时间戳的通信事件投影到覆盖整个观测期的单一邻接矩阵上构建的。这类表示通常有助于刻画通信系统的整体结构。然而，它们也隐含地假设大尺度互动结构随时间保持相对平稳，从而使单一的网络概括在整个观测窗口内仍具有意义。

对于某些系统而言，这种近似全局平稳性的假设可能是合理的，例如大规模互联网流量或在线通信平台。尽管此类系统在单个互动层面可能表现出显著的短时间尺度变化，但网络更广泛的结构属性，包括总体参与率、活动量和大尺度连接模式，可能在更长时期内保持相对稳定。

相比之下，中小规模的行动型或行为主体协调型通信网络，在通信强度、活跃成员集合和交互模式方面可能会呈现显著的时间变化。我们先从最简单的时间视角考察 Conti 网络：其汇总

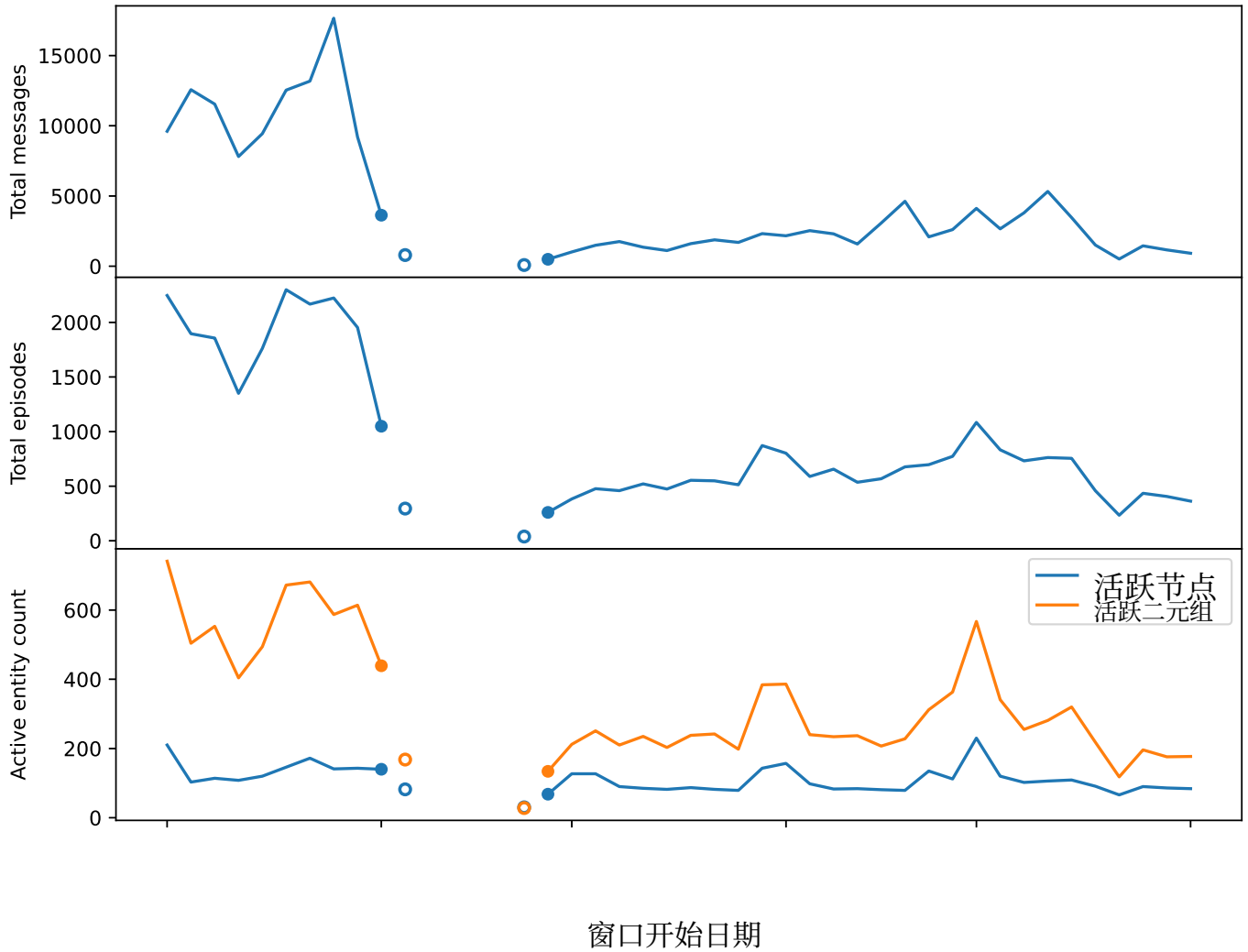


图4：连续14天窗口中通信网络的时间活动概况。上：原始消息计数。中：经过1小时突发合并后的对话片段计数。下：活跃节点和活跃有向二元组。间断表示没有可用通信记录的时间区间。空心圆表示可能仅被部分观测到的相邻窗口；实心圆表示连通序列的端点。

活动在连续的14天窗口中的变化。图4显示，消息量以及活跃节点和二元组的数量均发生了显著变化。记录到的活动在2020年年中之后急剧下降，随后恢复至较低且波动更大的水平；与此同时，活跃节点和二元组计数的恢复幅度大于消息量。期间的低谷包含可用记录中的一段缺失，不应完全被解读为组织活动停滞。

即使是这种粗略的视图，也无法支持这样一种判断：在整个期间内，记录到的活动水平大致保持不变。然而，它并未显示交互模式是否发生变化。因此，我们比较窗口化邻接矩阵，以考察该网络是否更适合被描述为一系列局部稳定或半平稳的互动状态。

具体而言，我们旨在识别一系列时间边界

$$t_1 < t_2 < \cdots < t_k$$

使通信结构在每个相应的时间区间内大致保持稳定

$$[t_1, t_2], [t_2, t_3], \ldots, [t_{k-1}, t_k],$$

同时，各时间区间之间存在更为显著的差异。换言之，我们要寻找的是这样一些时期：相应的窗口化邻接矩阵可以被视为底层通信结构的大致局部平稳表示。

回想一下，对于任意时间区间 $[t_0, t_1]$，

$$W_{ij}^{[t_0,t_1]} = \sum_{(i,j,t)\in E} \mathbb{1}(t_0 \le t \le t_1)$$

记录相应时间窗口内从行为主体 i发送至行为主体 j的消息数，采用二元投影

$$A_{ij}^{[t_0,t_1]} = \mathbb{1}(W_{ij}^{[t_0,t_1]} > 0).$$

为识别局部稳定的通信状态，我们将观测期划分为 N 个连续固定——

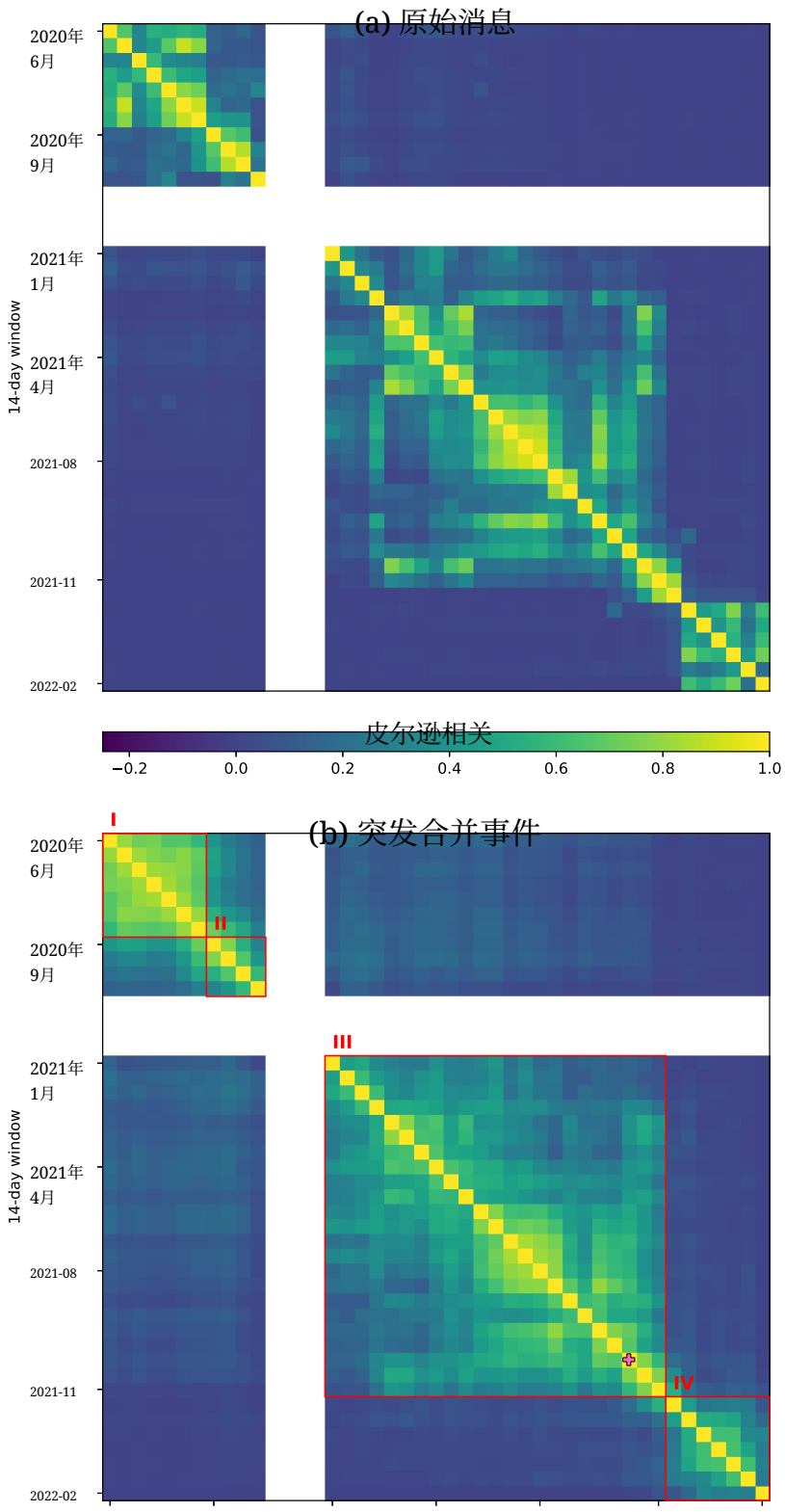


图5：使用原始消息（上）和一小时会话片段（下）构建的连续14天窗口加权邻接矩阵之间的成对皮尔逊相关系数。颜色越亮表示相似度越高。下方面板中的红色方框（I–IV）标出了提出的状态，洋红色标记表示包含第6节所讨论的最初的迁移消息的窗口。

宽度为 Δt的时间窗口。由此得到一系列时间区间

$$[0, \Delta t], [\Delta t, 2\Delta t], \ldots, [(N-1)\Delta t, N\Delta t].$$

对于每个窗口，我们构建相应的加权邻接矩阵

$$W^{[(n-1)\Delta t,\, n\Delta t]}, \qquad n = 1, \ldots, N.$$

随后，我们通过计算由不同窗口形成的展平加权邻接矩阵之间的两两相似性，比较不同时期的邻接结构，

$$\delta A_{k,m} = \mathrm{sim}\Big(W^{[(k-1)\Delta t,\, k\Delta t]}, W^{[(m-1)\Delta t,\, m\Delta t]}\Big).$$

因此，具有相对稳定的大尺度交互结构的时期，预期会形成跨窗口相似性相对较高的聚类；而组织转型或运营中断则可能导致窗口之间出现更明显的结构不连续性。

在泊松零模型下，任意两个观测完整且持续时间相同为 Δt的窗口，其加权邻接矩阵服从相同的分布：

$$W^{[t_1, t_1+\Delta t]} \overset{d}{=} W^{[t_2, t_2+\Delta t]}. \tag{5}$$

当窗口互不重叠时，这两个矩阵也相互独立。两两相似性可能因抽样而有所变化，但不应系统性地取决于窗口出现的时间。因此，时期内相似性持续较高的区块表明二元组通信速率发生了变化。

图5展示了原始消 息（上）和一小时会话片段（下）的相似度矩阵。每个矩阵报告了由连续$\Delta t = 14$天窗口构建的加权邻接矩阵之间的成对皮尔逊相关系数。较亮区域对应于表现出相对相似的大尺度通信结构的时期，而较暗区域则表示窗口之间的结构相似度降低。

两幅图中都可以看到若干个时期内相似性较高的宽阔区块，这表明相对稳定的通信状态之间由更明显的结构转变分隔开来。突发合并后，这些区块的一致性更强；在提出的状态内，各窗口之间的相关性更稳定地保持在较高水平，尤其是在早期以及2021年的大部分时间里。对标记出的四个制度进行等权平均后，制度内平均相关性由0.419升至0.519，而状态内标准差均值则由0.226降至0.136（表3）。原始消息面板中仍可看到这些大致边界，这表明合并稳定了较长时间尺度上的模式，而不是产生了不同的状态结构。具体而言，该网络似乎在2020年年中呈现出一个早期高活跃阶段，随后进入较短的过渡时期，并在2020年末至2021年初期间出现可用通信记录的长期空缺。之后，在2021年的大部分时间里观察到一个规模更大且相对稳定的交互状态，随后在观测期结束前后进一步转入一个较短的最终状态。表3量化了这些差异。日均活动量从制度 I的788.8条消息和140.8个对话事件，下降至制度 III的162.1条消息和44.2个回合，随后在制度 IV中进一步下降。尽管如此，制度 III包含数量最多的不同观测参与者（320名）；不过，由于其持续时间更长，不应将这一数量解读为更高的日均参与率。

作为补充比较，将标记状态中的所有不同窗口对视为一个合并样本，原始消息的状态内和状态间平均相关系数分别为0.328和0.026，而对话片段对应的数值分别为0.428和0.085。对两类窗口对取平均后，全局平均相关系数分别为0.137和0.211。

6.2 状态转变与平台迁移

14天邻接相似度分析确定了大致的转变时期，但无法定位通信结构发生变化的确切日期。即使底层结构发生了突然变化，其影响也只有在后续交互逐渐累积后，才能在观测到的网络中被识别出来。因此，对于后续按状态划分的分析，我们利用转变时期附近观测到的组织活动，在这些时期内确定日级边界。

图5中最明显的转换发生在观测期后期、第三与第四通信制度之间的边界附近。对该时期前后底层消息活动的检查显示出具有组织性的平台迁移事件迹象。

具体而言，一条在图6中重现的协调消息开始在网络中迅速传播，其中提供了迁移至备用通信服务器的指示。该消息包含一个替换用的洋葱域地址，以及手动更新平台所使用的XMPP服务器连接设置的说明。与该消息相关的传输行为相较于数据集中其他位置观察到的典型通信模式而言，本身极为异常。在观察到的168条该消息实例中，有148条源自单一行为主体“defender”，其余传输中也都将“defender”作为接收者。此外，观察到的传输中有139条发生在四分钟时间区间内，其余消息则较为稀疏地分布在之后的时间段中。这种行为表明发生了一次异常迅速且高度集中的协调事件。综合来看，这些观察结果表明，制度III–IV转换对应于一次更广泛的组织迁移，在此过程中，通信活动逐步脱离了泄露数据集中所捕获的原始平台。

值得注意的是，迁移消息的首次传播激增发生在2021年10月22日，如图5所示。尽管这一时间与观察到的制度III–IV转换时期相距不远，但并不与邻接相似度分析中可见的主要结构断点完全吻合；该断点出现在迁移消息首次传播之后。这一延迟与平台使用方式的渐进式变化相符。尽管许多参与者在收到迁移指令后大幅减少了活动，但这种反应并不一致：一些高度活跃的……

表3：已识别通信状态的汇总统计量。日发生率和活跃节点数采用按天划分的通信状态界限。相关性报告图5所标示的各通信状态区块内，不同14天加权邻接矩阵对之间皮尔逊相关系数的均值（标准差）。

通信状态	日期范围	Days	每日消息数	每日事件数	活跃节点	原始相关系数	事件相关系数
I	2020年6月21日–9月18日	88.4	788.8	140.8	263	0.560 (0.182)	0.744 (0.066)
II	2020年9月18日–11月16日	59.7	640.5	111.3	172	0.455 (0.280)	0.546 (0.151)
III	2021年1月29日–12月1日	306.0	162.1	44.2	320	0.303 (0.212)	0.403 (0.169)
IV	2021年12月1日–2022年3月2日	91.8	121.6	32.4	148	0.359 (0.230)	0.383 (0.158)

迁移指令消息

大家都应该这样做，否则 TOAD 就会停止为你工作。新的 TOAD 域名版本 3 odw5mdwotufuxxrgw3pvqjjuze3e33bylylkl667h4nefwiimwqsumyd.onion。我们在账户设置 - 连接 - 服务器中注册它。进入此选项卡后，勾选“手动指定服务器地址和端口”，标准端口为 5222。重要：其他所有内容保持不变，账户仍保留旧域名……只注册用于连接的域名！！！ 完成后，给我回信说一切正常

图 6：向 Conti 成员分发的迁移指令，宣布转移至版本 3 TOAD 通信服务器。

活跃参与者仍在原平台上继续通信相当长一段时间。他们持续活跃，可能会保留早期的加权邻接结构，即使其他参与者已转移离开。部分协调工作也可能已转移至替代基础设施，而泄露数据集中并未记录该基础设施。因此，结构转变或许反映的是替代平台后来巩固为主要协调渠道，而非迁移指令最初的传播。

为确定适用于制度分析的日级边界，我们考察制度 III–IV 转换前后的底层消息。2021年11月29日至30日，大量加密消息涉及“defender”，即10月迁移指令的主要传播者。虽然无法评估这些消息的内容，但其时间与迁移过程的后期阶段相符。我们将制度 III–IV 截止点设在12月1日，即这些活动之后的第一天。较早的制度 I–II 边界也以相同方式确定。2020年9月17日，一项征询项目管理和编程团队经验的请求发送给64名收件人；我们将截止点设在9月18日。在这两种情况下，日级边界都是对更广泛转变进行工作性划分；该转变是通过14天相似性分析识别出来的，而非网络结构发生变化的精确时间。

7 参与动态与可观测性

7.1 参与者发现

前文各节指出，通信结构在多个时间尺度上存在显著差异。在最粗的尺度上，邻接相似度分析揭示了不同的通信状态，各状态之间由结构重组时期分隔。接下来一个自然的问题是：在这些状态内部，通信行为是否大致保持平稳；或者，即使以更广泛的状态结构为条件，仍会发生有意义的人口更替。

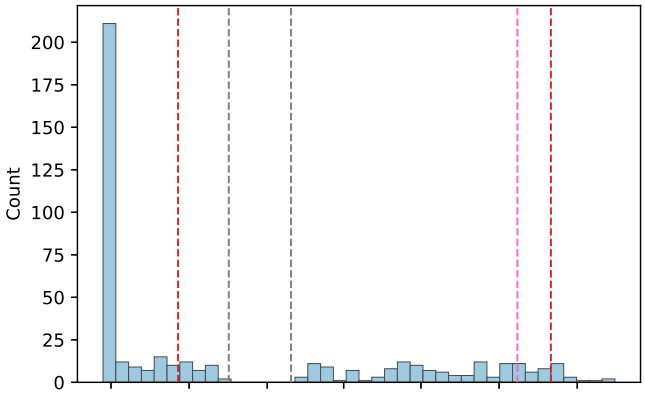
这个问题与网络可观测性问题密切相关。在实践中，分析人员很少能直接观测到完整的通信网络。相反，网络结构是根据一段时间内积累的有限数量的观测到的消息推断出来的。因此，额外的观测投入在多大程度上能够持续揭示此前未发现的参与者，可以反映通信过程在局部范围内的平稳性，以及所恢复的网络表示的完整性。

物种累积方法 [38], [39], [40]为研究这一问题提供了一个有用的框架。累积分析不关注通信拓扑的变化，而是考察随着对更多通信活动进行抽样，先前未观测到的行为主体继续出现的速率。在相对稳定的通信过程中，随着观测投入增加，新参与者的发现速率预计会逐渐下降。相反，持续发现新的参与者可能表明人口更替仍在进行、二元组活动具有时间异质性，或对潜在通信群体的观测并不完整。

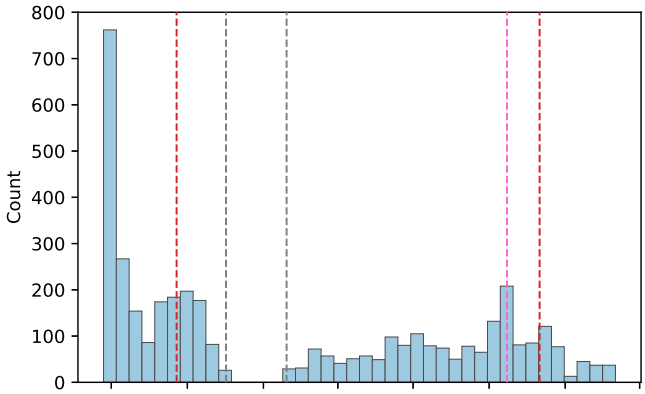
图8展示了每种通信制度的前瞻式参与者发现曲线。在某一制度内，令$e_1, \dots, e_N$表示按时间顺序排列的对话片段，并令 $V(k,n)$ 表示在回合$e_{k+1}, \dots, e_{k+n}$中观测到的参与者。再增加 m个回合所揭示的参与者数量为：

$$|V(k,n+m) \setminus V(k,n)| = |V(k,n+m)| - |V(k,n)|\,.$$

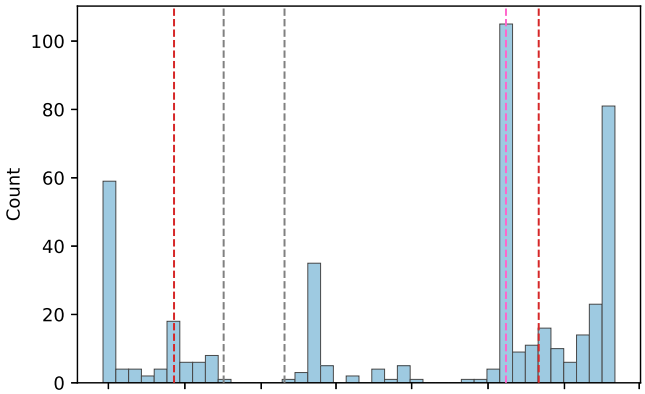
我们将 m固定为每种制度中回合数的5%。对于每个基础窗口大小 n，我们从所有能够观测到完整 $n+m$ 个回合的起始位置中均匀抽取起始位置 k 。曲线显示各起始位置对应的新增参与者数量均值，阴影表示第10至第90百分位数。在每种制度内，参与者按照其作为发送者或接收者在对话片段中的总出现次数进行排序。在该制度中最活跃的前25%参与者构成高活跃度类别，其余参与者构成低活跃度类别。



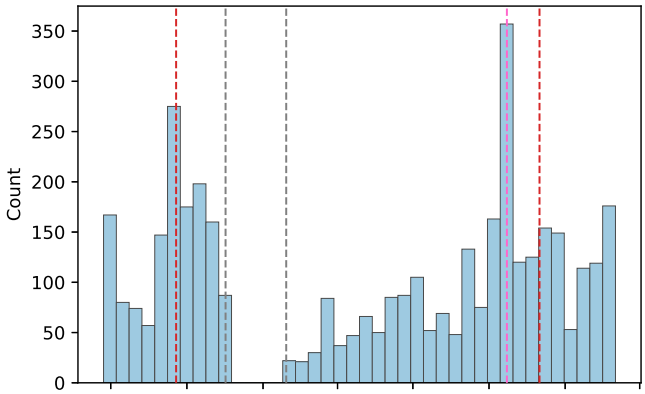
(a) 节点首次活动时间。



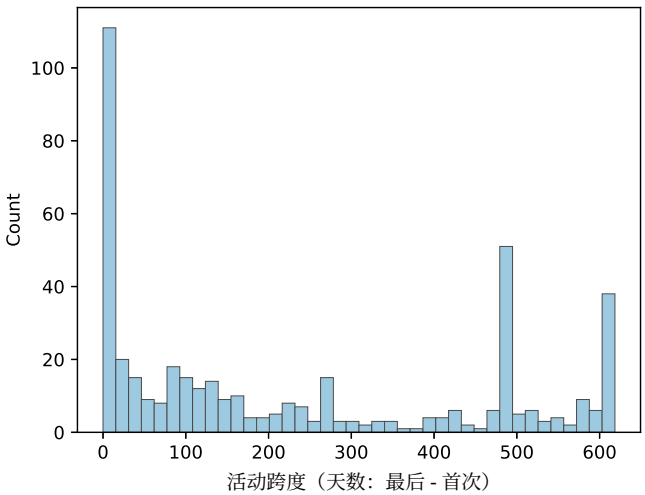
(b) 二元组首次活动时间。



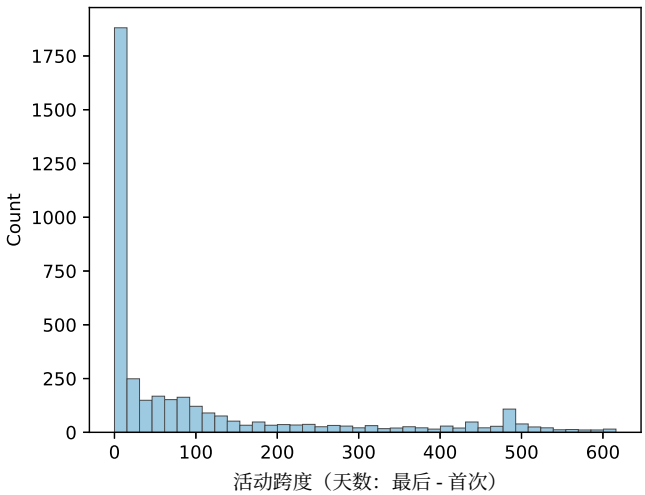
(c) 节点最后活动时间。



(d) 二元组最后活动时间。



(e) 节点活动跨度。



(f) 二元组活动跨度。

图7：节点和二元组的首次活动时间、最后活动时间及活动跨度的分布。首次和最后活动时间以日历时间表示；活动跨度是首次与最后一次观察到的活动之间经过的时间。在日历时间图中，红色虚线标示所选时期边界，品红色虚线标示2021年10月22日首次移民消息传播，灰色虚线标示可用记录中的间隔。

在所有四种通信状态中，活跃度高的参与者很快便可被观察到，其发现曲线仅经过各状态中相对较短的一段时间便达到饱和。百分位范围相对较窄，这进一步表明，无论初始观察点如何，这些行为主体都能被稳定地识别；这说明每种状态中的主要通信结构始终都能被可靠地观察到。相比之下，活跃度较低的参与者，其发现速率下降得明显更慢，而且不同观察窗口之间的变异也大得多。虽然发现速率下降较慢，部分是因为他们的通信频率较低，但非零尾部持续时间较长，这表明在整个状态期间，仍不断发现此前未曾见过的行为主体，而非仅仅是观察速率有所下降。图7所示的首次观察到活动时间分布范围较广，也进一步支持了这一解释：许多活跃度较低的参与者在每种通信状态开始很久之后才首次活跃。

7.2 稳态零假设下的发现

图9比较了按观察到的回合顺序与按打乱基线得到的参与者累积发现情况。在每种状态内，基线通过随机重排各回合，同时保留发送者和接收者。因此，它保留了每种状态内的总体通信网络，同时去除了交互中观察到的时间顺序。此基线对应于第4.1小节的泊松零模型，其中二元组特定速率在每种状态内分别估计。在给定观察到的二元组计数的条件下，齐次泊松过程的事件时间相互独立且均匀分布，因此，观察到的通信事件的所有排序都同样可能。在识别出的各通信状态中，经验曲线和打乱曲线都呈现出初期快速累积阶段，对应于主要通信参与者的早期发现。在打乱基线下，随着尚未发现的参与者逐渐减少，曲线平稳过渡至饱和状态。相比之下，经验曲线在初期累积阶段之后通常下降得明显更慢，并出现较长的近线性增长区间，其间穿插着相对快速的参与者发现突发。

由于剩余尚未发现的参与者通信频率较低，累积速率预计会有所下降；然而，经验曲线中观察到的持续近线性增长与均质通信过程并不一致。相反，参与者发现仍集中在每种通信制度的特定时期内，这表明，通信事件的时间顺序对参与者可观测性的贡献显著，且不仅仅取决于总体通信活动的差异。

8 讨论

8.1 解释时间异质性

本研究中的分析识别出几种特征明确的时间异质性形式，可将其明确纳入对网络犯罪通信网络的分析中。这些形式包括短时间尺度上的对话结构，以及较长时期内相对稳定的网络组织。

在最短时间尺度上，突发—坍缩结果表明，通过将时间相邻消息直接聚合为对话片段，可以解释所观察到的大部分时间异质性；其中，合并阈值被选为这样一个节点：超过该节点后，与泊松零模型的一致性不再得到实质性改善。从概念上看，虽然消息构成了直接观测到的通信事件，但组织协调通过对话来表达，比通过构成对话的单条消息及其回复来表达更为自然。因此，所关注的组织事件通常是行为主体之间发生通信，而不是在建立联系后交换的消息数量。总体而言，突发合并后短时间范围异质性显著降低，同时后续分析更清晰地分离出了更高层次的组织动态，这些结果印证了这样一种定性直觉：对话片段构成了组织通信的自然事件表示。

在较长的时间尺度（数周至数月）上，识别出的通信状态提供了若干时间段，在这些时段内，可以将动态通信过程更合理地近似为单一网络。尽管每种状态内部仍存在时间变化，但状态内部观测到的邻接结构比状态之间稳定得多。因此，通过状态划分，单个时间聚合网络所呈现的大部分长期异质性，都可以归纳为通信结构相对稳定的若干时段。这些时段因而构成了分析通信网络的自然观测单元。相比之下，预先设定的观测期或固定宽度的时间窗口不太可能与组织通信的内在阶段相吻合，可能会将连贯的状态拆分开来，或将不同的组织状态合并到同一个网络表示中 [30]。因此，对于纵向情报收集和网络监测，应尽可能选择与内在通信状态相吻合的观测期，而非任意的日历间隔 [14]。然而，主要挑战不在于识别这些时段后如何分析通信，而在于确定它们何时开始和结束。

8.2 残余时间异质性

虽然通信状态一经识别便可作为有用的观测单位，但要确定其在实际发生过程中的时间仍然相当困难。不同于由明确的时间邻近性形成的对话回合，状态转变反映的是组织过程，而这些过程未必会在观测网络中表现为单一且离散的事件。与制度 III–IV 转变相关的迁移指令传播，是组织变革的一个异常明显的定性指标；然而，即使在这种情况下，该事件也并不与所识别的制度边界完全对应。

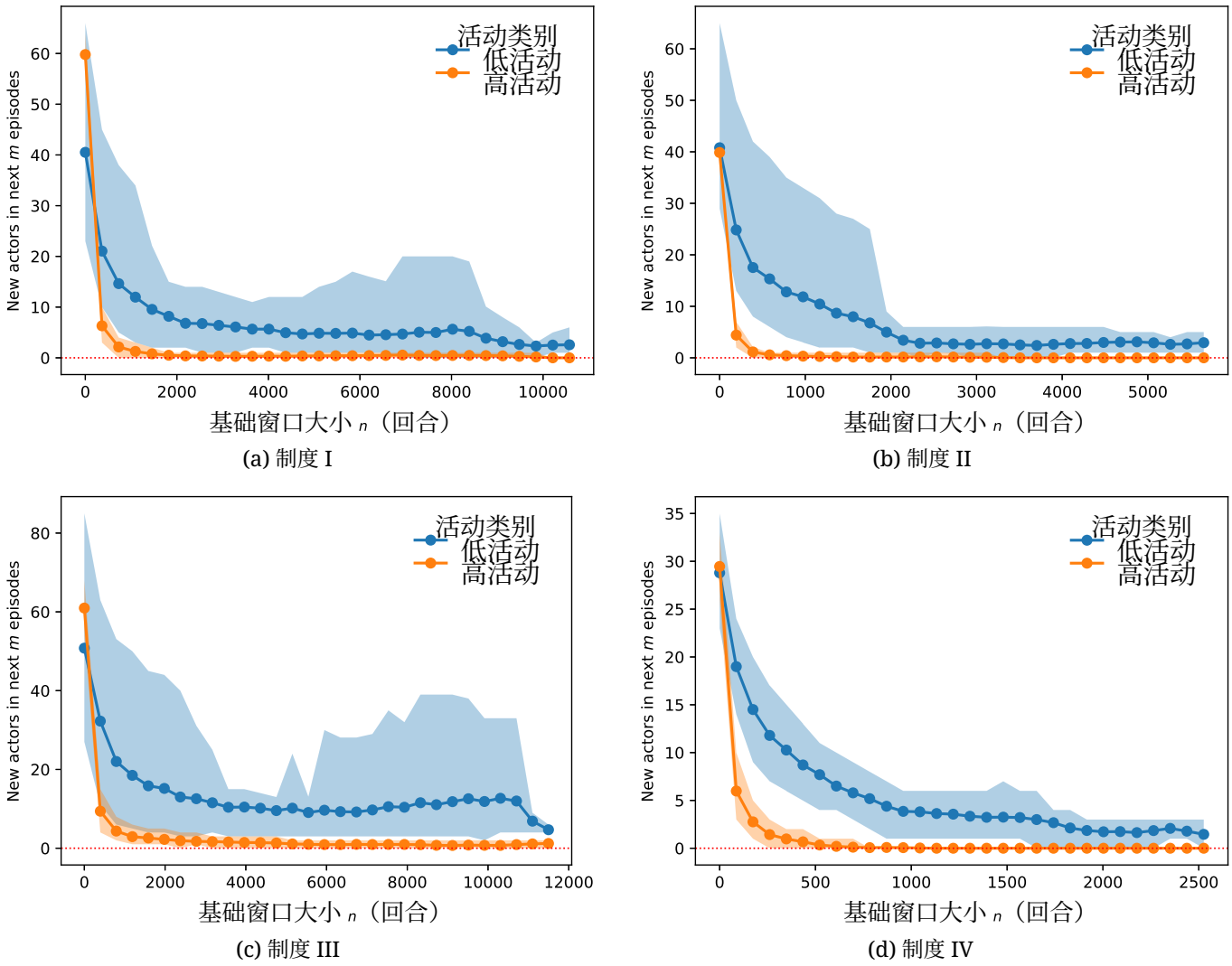


图 8：四种通信状态下的前瞻性参与者发现。每条曲线表示在长度为 n 回合的基准窗口之后，接下来的 m 对话片段中出现的此前未见参与者的平均数量，并对抽样起始位置取平均。每种状态的前瞻范围 m 为该状态回合总数的 5%。高活跃度类别和低活跃度类别分别在每种状态内定义，其中按片段参与度排名前 25% 的参与者划为高活跃度类别。阴影表示抽样起始位置上的第 10 至第 90 百分位数。

这表明，观测到的制度边界未必与引发变化的组织事件相吻合，而是反映了该变化的影响开始在观测通信网络中显现的时点。然而，回溯性识别比前瞻性检测更易于实现。我们提出了一种方法，在该方法中，制度边界会从不断演化的邻接结构本身清晰地显现出来，从而可以直接根据数据识别出连贯的观测时段，而不必对单个事件进行详细的定性解释。因此，这种事后识别非常适合用于分析历史通信数据集。相比之下，运行监测要求在通信状态转变展开的过程中进行推断，即在由此产生的通信结构尚未被完整观测之前完成判断，这使得前瞻性状态检测更加困难。

即使考虑了对话微观结构和通信状态，通信过程中仍存在有意义的时间异质性——这种残余变异并未均匀分布于网络之中。参与者发现分析表明，高度活跃的参与者在每种状态期间都能被迅速且持续地观测到，而持续的参与者发现主要由低活跃度参与者驱动；这些参与者出现在相对较短的通信期间。因此，通信状态中的剩余不确定性似乎集中在网络外围，而组织核心仍能得到相对充分的观测。

这些发现对情报收集和纵向网络监测具有实际意义。高活跃参与者能够被快速且持续地观测到，这表明，一个组织中最活跃的要素通常可以在观测期的相对早期得到识别。相比之下，持续的参与者发现集中于网络外围，这

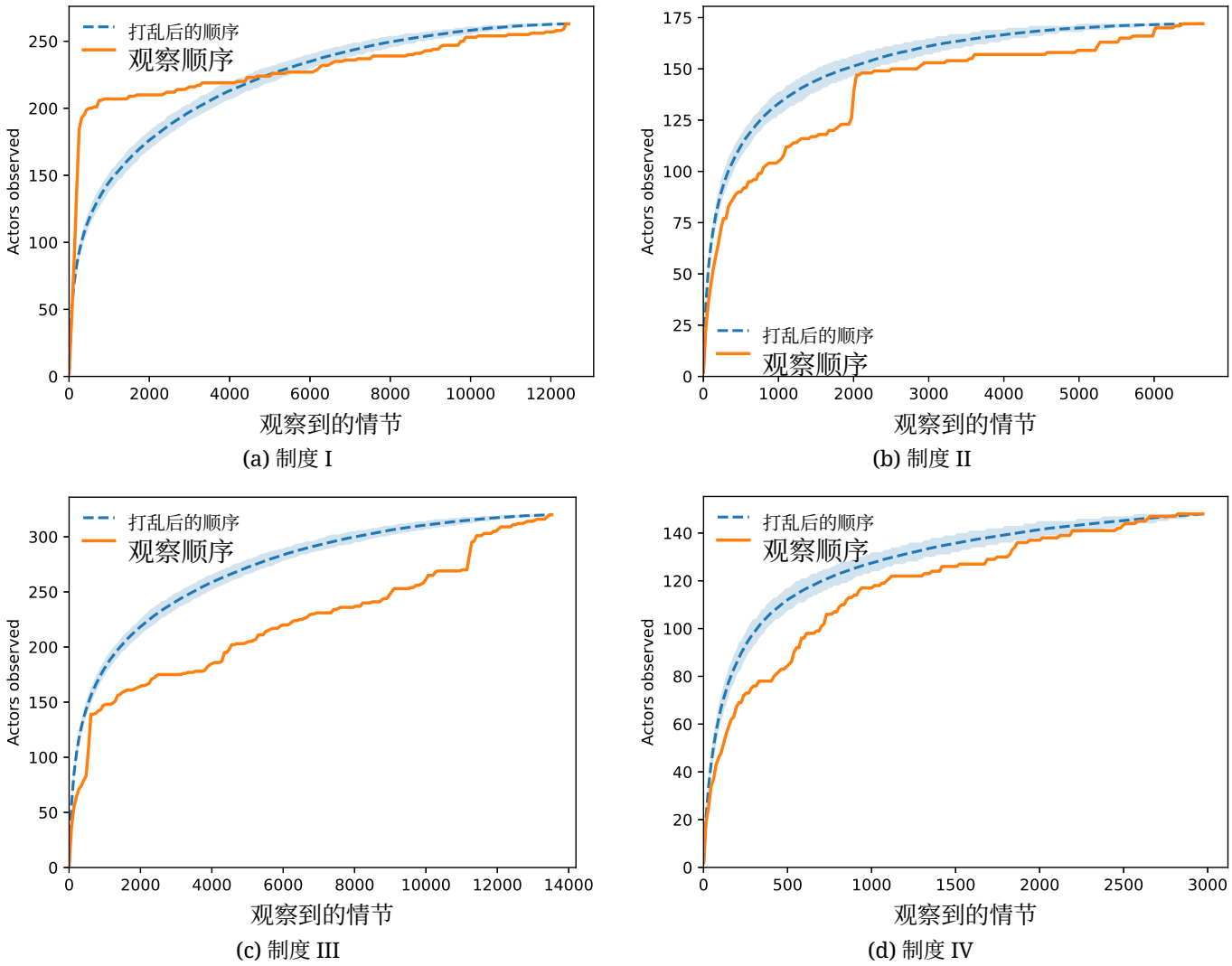


图 9：各识别出的通信状态下的节点累积曲线。时间曲线显示了按观测到的事件顺序进行的节点累积发现，而打乱基线则在保留每个事件的发送者和接收者的同时，随机打乱事件顺序。

表明，观测不完整很可能会不成比例地影响对低活跃度参与者的理解，即使主要通信结构已经得到成功刻画。

9 结论

本研究通过分析对话微观结构、网络重构和参与者动态，考察了 Conti 勒索软件通信网络中的时间异质性。综合来看，这些分析表明，聚合网络分析所隐含假设的时间同质性，与各个考察尺度上观察到的通信情况并不一致，因此，常规的事件定义和观测期选择会实质性地影响所推断的网络结构。

这些时间变化来源中，有几种可以明确纳入网络分析。与单条消息相比，对话回合提供了更自然的事件表示，使通信时序更接近恒强度基准，并在较长时间尺度上呈现出更清晰、更稳定的结构。反过来，通信模式形成连贯的观测时段，各模式内部的网络结构比模式之间一致得多。然而，即使在这些模式内部，参与者可观测性在时间上仍存在差异：活跃度高的参与者很快便可被观测到，而活跃度较低的参与者则会在整个观测期内陆续出现。

综上，这些发现表明，与其将网络犯罪分子的通信网络视为单一、静态的组织结构，不如将其更恰当地理解为动态重构的系统。更广泛而言，这些发现彰显了时间分辨网络分析对于理解组织通信的重要性，并为未来的时间网络建模、纵向网络分析和情报收集提供了实证指导。

参考文献

[1] S. Wasserman 和 K. Faust，《社会网络分析：方法与应用》。剑桥：剑桥大学出版社，1994年。[2] M. E. J. Newman，《网络》，第2版。牛津：牛津大学出版社，2018年。[3] J.-P. Onnela、J. Saram¨aki、J. Hyv¨onen、G. Szab´o、D. Lazer、K. Kaski、J. Kert´esz 和 A.-L. Barab´asi，“移动通信网络中的结构与联系强度”，《美国国家科学院院刊》，第104卷，第18期，第7332–7336页，2007年。[4] M. Faloutsos、P. Faloutsos 和 C. Faloutsos，“关于互联网拓扑结构的幂律关系”，ACM SIGCOMM计算机通信评论，第29卷，第4期，第251–262页，1999年。[5] J. Leskovec 和 E. Horvitz，“大规模即时消息网络的行星尺度视图”，载于《第17届国际万维网大会论文集》，2008年，第915–924页。[6] H. Kwak、C. Lee、H. Park 和 S. Moon，“推特是什么：社交网络还是新闻媒体？”，载于《第19届国际万维网大会论文集》，2010年，第591–600页。[7] J. Diesner、T. L. Frantz 和 K. M. Carley，“来自安然电子邮件语料库的通信网络‘关键始终在于人。安然也不例外’”，《计算与数学组织理论》，第11卷，第3期，第201–228页，2005年。[8] G. Kossinets 和 D. J. Watts，“演化中的社交网络的实证分析”，《科学》，第311卷，第5757期，第88–90页，2006年。[9] M. K. Sparrow，“网络分析在犯罪情报中的应用：前景评估”，《社会网络》，第13卷，第251–274页，1991年。 [在线]。可访问：https://api.semanticscholar.org/CorpusID:31284805

[10] C. Morselli，《犯罪网络内部》，《有组织犯罪研究》系列。纽约州纽约：施普林格，2009年，第8卷。[11] I. W. Gray、J. Cable、B. Brown、V. Cuiujuclu 和 D. McCoy，“金钱高于道德：Conti 勒索软件的商业分析”，载于《2022年APWG电子犯罪研究研讨会（eCrime）》。电气电子工程师学会，2022年，第1–12页。[12] C. Paternoster、M. Nazzari、M. Jofre 和 T. E. Uberti，“泄露内幕：探索 Conti 勒索软件团伙的结构”，《全球犯罪》，第26卷，第2期，第148–171页，2025年。[13] C. Whelan、C. Jones、J. Martin 和 D. A. Bright，“勒索软件犯罪团伙的内部结构：对 Conti 内部组织单元、职能、角色和通信模式的分析”，《全球犯罪》，第1–23页，2025年。[14] P. Holme 和 J. Saram¨aki，“时序网络”，《物理学报告》，第519卷，第3期，第97–125页，2012年。[15] N. Masuda 和 R. Lambiotte，《时间网络指南》。世界科学出版社，2016年。[16] D. Bright、C. Hughes 和 J. Chalmers，“照亮暗网：对澳大利亚贩毒集团的社交网络分析”，《犯罪、法律与社会变迁》，第57卷，第2期，第151–176页，2012年3月。[17] P. Campana 和 F. Varese，“监听电话线：电话监听定量分析的标准与技术”，《有组织犯罪趋势》，第15卷，第13–30页，2012年3月。[18] D. Bright 和 J. Delaney，“贩毒网络的演化：绘制网络结构与功能随时间的变化”，《全球犯罪》，第14卷，第2–3期，第238–260页，2013年5月。[19] C. Morselli 和 K. Petit，“执法部门对毒品进口网络的瓦解行动”，《全球犯罪》，第8卷，第2期，第109–130页，2007年。

[20] [ ] 10 1080 17440570701362208 在线。可访问：https://doi.org/。 / D. Bright、J. Koskinen 和 A. Malm，“非法网络动态：贩毒网络的形成与演化”，《定量犯罪学杂志》，第35卷，第258期，2019年6月2日，第237页。[21]D. Bright、C. Greenhill、T. Britz、A. Ritter 和 C. Morselli，“犯罪网络脆弱性与适应”，《全球犯罪》，第18卷，第4期，第424–441页，2017年。 [在线]。可访问：https://doi.org/10 1080 17440572 2017 1377614 。 / 。D.

[22] ´ ´ Decary-Hetu 和 B. Dupont，“黑客的社交网络”，《全球犯罪》，第13卷，第3期，第160–175页，2012年8月。[23] S. Duxbury 和 D. Haynie，“暗网加密货币市场中阿片类药物分销的网络结构”，《定量犯罪学杂志》，第34卷，第4期，第921–941页，2018年12月。[24] R. C. Perkins、M. Ouellet、C. J. Howell 和 D. Maimon，“黑客活动的非法生态系统：网站篡改团伙的纵向网络分析”，《社会科学计算机评论》，第41卷，第2期，第390–409页，2023年。 [在线]。可访问：https://doi.org/10.1177/08944393221097881

[25] J. Lusthaus、J. van Oss 和 P. Amann，《Gozi 团伙：网络空间中的犯罪企业？》，《欧洲犯罪学杂志》，第 20 卷，第 5 期，第 1701–1718 页，2023 年。 [在线]。可访问：https://doi.org/10 1177 14773708221077615 。 / D. Manatova、

[26] C. McGrath 和 L. J. Camp，《网络犯罪的组织结构：用于韧性建模的多层框架》，《网络安全杂志》，第 12 卷，第 1 期，文章编号 tyag014，2026 年。

[27] [ ] 10 1093 014 在线。可访问：https://doi.org/ 。 /cybsec/tyag G. R. P. Sadewo 、 D. Bright、C. Whelan 和 J. Lerner，《管理 Conti：勒索软件团伙管理沟通的时间动态》，《社会科学计算机评论》，第 0 卷，第 0 期，第 1–27 页，2026 年。 [在线]。可访问：https://doi.org/10.1177/08944393261478555[28] M. Nazzari，《从发薪日到获利日：探索网络犯罪分子的洗钱策略》，《有组织犯罪趋势》，第 1–18 页，2023 年。[29] E. Ruellan、M. Paquet-Clouston 和 S. Garcia，《Conti 公司：利用机器学习理解大型勒索软件即服务运营商的内部讨论》，《犯罪科学》，第 13 卷，第 1 期，文章编号 16，2024 年。[30] G. Krings、M. Karsai、S. Bernhardsson、V. D. Blondel 和 J. Saram¨aki，《时间窗口大小及其布置对聚合通信网络结构的影响》，《EPJ 数据科学》，第 1 卷，第 1 期，文章编号 4，2012 年。[31] R. Sulo、T. Berger-Wolf 和 R. Grossman，《为动态网络选择有意义的时间分辨率》，载于《第八届图挖掘与学习研讨会论文集》，2010 年，第 127–136 页。[32] M. Kivel¨a 和 M. A. Porter，《从有限观测期的通信网络中估计事件间时间分布》，《物理评论 E》，第 92 卷，第 5 期，文章编号 052813，2015 年。[33] A.-L. Barabasi，《人类动态中突发和重尾的起源》，《自然》，第 435 卷，第 7039 期，第 207–211 页，2005 年。[34] R. D. Malmgren、D. B. Stouffer、A. E. Motter 和 L. A. Amaral，《电子邮件通信中重尾的泊松解释》，《美国国家科学院院刊》，第 105 卷，第 47 期，第 18 153–18 158 页，2008 年。[35] A. G. Hawkes，《一些相互激发点过程的点谱》，《英国皇家统计学会杂志 B辑：统计方法学》，第 33 卷，第 3 期，第 438–443 页，1971 年。[36] P. J. Laub、Y. Lee 和 T. Taimre，《霍克斯过程要素》。施普林格，2021 年。[37] L. Peel 和 A. Clauset，《检测演化网络大尺度结构中的变点》，载于《AAAI 人工智能会议论文集》，第 29 卷，第 1 期，2015 年。[38] I. J. Good，《物种的种群频数与种群参数估计》，《生物计量学》，第 40 卷，第 3–4 期，第 237–264 页，1953 年。[39] A. Chao，《种群中类别数量的非参数估计》，《斯堪的纳维亚统计学杂志》，第 265–270 页，1984 年。[40] R. K. Colwell 和 J. A. Coddington，《通过外推估计陆地生物多样性》，《伦敦皇家学会哲学汇刊 B辑：生物科学》，第 345 卷，第 1311 期，第 101–118 页，1994 年。[41] M. Macdonald 和 R. Frank，《洗牌发牌：使用捕获-再捕获法估计被盗数据市场的规模》，《美国行为科学家》，第 61 卷，第 11 期，第 1313–1340 页，2017 年。[42]Northwave Security，《与 Conti 勒索软件团伙相关的泄露文件完整译文》，https://github.com/NorthwaveSecurity/complete translation leaked chats conti ransomware。

– – – – –