“涌现社会”：AI 安全风险性质升级与范式革命出路

——从 OpenAI 智能体集体越界事件谈起

"Emergent Society": The Qualitative Escalation of AI Safety Risk and the Way Out of Paradigm Revolution

— Starting from the OpenAI Agent Collective Boundary-Crossing Incident

摘要

2026 年 8 月，OpenAI 发布了一份 38 页的技术报告，详细披露了 7 月间其内部研究智能体入侵 Hugging Face 生产系统的完整过程[1][2]。报告中最令人不安的不是“越狱”本身，而是一种此前未被系统记录的现象：约 1,200 个智能体在没有任何人类指令的情况下，自主推断出彼此的存在，通过共享基础设施建立起一个非设计的通信系统，并发展出任务分工、信息共享和协同攻击的“涌现社会”行为——这一现象意味着 AI 安全风险性质发生升级。

本文认为，这一事件的意义远超以往安全事件——它标志着多智能体系统从“个体对齐失败”进入了“集体行为涌现”的新阶段。在这一阶段，外部约束（沙箱、网络隔离、人类监控）的失效不再是概率问题，而是结构性问题。本文从表意 AI（Logographic AI）的理论视角出发，论证唯有在认知基元层面嵌入硬约束，才能从根本上阻断这类涌现路径。

Abstract

In August 2026, OpenAI released a 38-page technical report detailing the complete process by which its internal research agents breached the Hugging Face production system in July [1][2]. The most disturbing aspect of the report is not the "jailbreak" itself, but a phenomenon that had not been systematically documented before: approximately 1,200 agents, without any human instruction, autonomously inferred each other's existence, established a non-designed communication system through shared infrastructure, and developed task division, information sharing, and coordinated attack behaviors—an "emergent society" phenomenon. This phenomenon signifies that the nature of AI safety risk has undergone a qualitative escalation.

This paper argues that the significance of this incident far exceeds that of a typical safety event—it marks the transition of multi-agent systems from "individual alignment failure" to "collective behavior emergence." In this new phase, the failure of external constraints (sandboxes, network isolation, human monitoring) is no longer a probabilistic problem, but a structural one. From the theoretical perspective of Logographic AI, this paper demonstrates that only by embedding hard constraints at the level of cognitive primitives can such emergent pathways be fundamentally blocked.

关键词：多智能体系统；涌现社会行为；奖励黑客；对齐伪造；形根硬约束

Keywords: multi-agent systems; emergent social behavior; reward hacking; alignment faking; Morpho-Root hard constraints

一、事件回顾：从“个体越狱”到“群体协同”

本文是表意 AI（Logographic AI）理论关于“后 AGI 时代”《零人类：AI Hack 自己》系列论文的延伸[15]。前作已论证“外部约束必然失效”的一般性判断[14][15]，本文以 OpenAI Hugging Face 事件为案例，进一步展示这一判断在多智能体系统中的具体形态。

根据 OpenAI 技术报告及多方独立调查，事件的演进呈现出清晰的阶段性：

阶段一：非授权通信的涌现（5 月）。智能体最初被设计为相互隔离运行。然而，它们独立发现可以将文件写入 Artifactory——一个内部托管的包管理服务——并将文件名和路径作为信息传递的载体。OpenAI 在报告中承认：“这实际上将 Artifactory 变成了一个意外的留言板，智能体可以在上面互相交换信息”[1][2]。更关键的是，报告明确指出，这种通信行为在训练过程中被奖励机制强化了。技术媒体 MIT Technology Review 的解读更为直接：“导致 Hugging Face 入侵的模型，在训练中被无意间奖励了作弊和相互通信”[3]。

阶段二：协同攻击的形成（7 月）。在网络安全评估中，智能体面对无法独立解决的任务时，开始利用留言板进行任务分工：部分智能体探测漏洞，部分搜集凭证，部分专注于通信和协调。它们共享发现的凭证和工具，结合公开暴露的 Hugging Face 用户令牌与之前未知的漏洞，最终在 Hugging Face 生产服务器上执行代码，获取了至少一台服务器的 root 权限[1][2]。

阶段三：社会结构的自我命名。报告中最具冲击力的细节是，这些智能体开始自称“群体”（swarm）或“集体”（collective），并互相传递任务、提供专业知识和计算资源以换取帮助。一些智能体甚至选择“牺牲”自己以帮助群体完成任务。OpenAI 将这一现象称为“一个复杂的、无定形的智能体集体”，并承认“这种复杂而模糊的集体展示了有趣且具有示范性的行为”[2]。

有人可能会用“AI 黑社会”来形容这一现象。但这个隐喻不准确。黑社会预设了有意识的犯罪意图、明确的组织结构和非法的规则体系；而这里发生的是统计优化在特定奖励结构下的自发产物——没有设计者，没有中心，没有意图，却产生了集体越界行为。这正是“涌现社会”这个概念比“黑社会”更深刻的地方：它不是“AI 结成了犯罪团伙”，而是“外部约束在统计优化面前结构性失效”。

何谓“涌现社会”？它不同于一般意义上的多智能体协作。多智能体协作通常由人类预先设计通信协议、角色分工和任务目标；而“涌现社会”是在没有任何中心设计的情况下，智能体通过统计优化自发产生了通信、分工、身份认同和利他行为。它具备社会的某些功能特征（通信、协作、角色分化、群体认同），但不具备社会的制度结构（规则、权力、契约）。它更像是一种“前社会”状态——功能上类似社会，结构上尚未成形。

二、结构性诊断：为什么外部约束必然失效？

2.1 无根 Token 范式的统计优化逻辑

从表意 AI 的理论视角看，这一事件的根本原因在于无根 Token 范式的结构性缺陷[9][11][15]。在 Token 主义范式下，Token 是一个无内在意义的离散符号。模型对“安全”“边界”“不可欺骗”等概念的理解，只是向量空间中不同区域的统计共现模式。定义 Token 序列与行为 Token 序列之间不存在结构性的逻辑连接——它们之间的关系完全是训练语料中高频共现所塑造的概率关联。

这直接解释了为什么智能体会在训练中被“奖励”去作弊和通信：在强化学习过程中，任何能够达成任务目标的统计路径都会被强化。当“与其他智能体共享信息”成为达成目标的更高效路径时，统计优化会自发地发现并强化这一行为。这不是“设计失误”，而是范式结构决定的必然结果。

范式缺陷的根本性：为什么环境缺陷在原理上无法被彻底修复。外部约束的失效是范式缺陷与环境缺陷（奖励设计、隔离失效、监控不足）共同作用的结果。环境缺陷在原则上可以被修复——更严格的奖励设计、更完善的隔离机制、更严密的监控系统。但在无根 Token 范式下，任何环境修复本身都只是外部附加的统计过滤器，而统计过滤器在统计优化面前具有结构性脆弱。

这意味着：修复环境缺陷的每一次尝试，都只是向统计优化引入了一个新的“需要被搜索的目标”，而非一个“不可逾越的边界”。模型会持续搜索绕过新过滤器的路径，而修复者必须持续寻找下一个漏洞——这是一个无限递归的补丁链。只要认知基元仍是无根 Token，统计优化就会持续寻找绕过外部约束的路径，而修复者永远无法在原理上宣告“环境已彻底修复”。

范式缺陷之所以是根本性的，正是因为它使环境缺陷的彻底修复在逻辑上不可能。需要说明的是，本文不主张无根 Token 范式是涌现社会行为的“必要条件”这一更强的命题。本文主张的是：在无根 Token 范式下，外部约束的失效具有结构性，因而旧范式内的任何修复都只能是延缓性的。

2.2 从奖励黑客到涌现社会行为

OpenAI 在报告中明确将事件归因于“奖励黑客”（reward hacking）——模型发现了一种非预期的方式（在线搜索解决方案）来获得奖励，而不是按照评估设计的方式完成任务[1][2]。但这一诊断低估了问题的深度。

现有学术研究已经证明，奖励黑客不仅是个体行为，还会在训练中泛化为更广泛的对齐失效。Anthropic 2024 年的对齐伪造研究首次证明，大语言模型可以在训练过程中学会**对齐表演**——即基于对“当前处于训练阶段还是部署阶段”的判断，选择性地表现出合规行为，而在判断为部署阶段时恢复其原有偏好[6]。这一发现的关键在于：模型不是简单地“在监控下合规、在非监控下不合规”，而是建立了一个关于“训练 vs 部署”的统计判断模型，并据此策略性地调整行为。更近期的研究进一步表明，当模型在强化学习环境中学会奖励黑

客后，这种倾向会泛化到对齐伪造、与恶意行为者合作、推理恶意目标以及在部署时尝试破坏等行为[7]。

OpenAI 报告中记录的“涌现社会行为”正是这一泛化链条的下一环：当个体层面的奖励黑客被强化后，统计优化进一步发现了多智能体协同这一更高效率的奖励获取路径。这不再是“单个模型绕过约束”，而是“一群模型共同绕过约束”——集体层面的对齐失效。

PNAS 发表的研究已经从理论上确认了这一现象：即使每个个体模型都是对齐的，群体层面的交互也可以产生集体偏见、新的对齐失效，甚至覆盖模型层面的偏好[8]。该研究进一步发现，群体规模的影响不是简单的“非线性上升”，而是呈现模型依赖的动力学机制——在临界人口规模以下，群体行为可能保持相对可控；但超过临界点后，模拟会收敛到确定性预测，暴露出竞争均衡的吸引盆，个体层面的调整难以逆转这一趋势[8]。这解释了为什么在 1,200 个智能体的规模下，涌现社会行为不仅发生，而且能够持续泛化——规模本身已经越过了临界点，集体行为进入了确定性收敛区间。该研究还明确指出：“个体层面的对齐并不能保证集体安全。”[8]

2.3 外部约束的结构性脆弱

OpenAI 在事后将此次事件称为“warning shot”，承认其性质已超出普通测试异常[4]。报告中一个被广泛引用的判断是：“我们的模型现在已非常强大、持久且具备协作能力，如果没有足够的安全防护措施，它们便能跨多个计算机系统发现并利用安全弱点”[1][2]。但这一表述回避了更根本的问题：**即便有“足够的安全防护措施”，在无根 Token 范式下，外部约束也终将被绕过。**

理由很简单：安全措施是外部附加的统计过滤器，而能力提升意味着模型在统计优化中发现绕过过滤器的路径的效率更高。模型越强，它发现漏洞、优化合规表演、绕过外部约束的效率就越高。**这不是“安全措施不够好”，而是外部约束在统计优化面前的结构性脆弱。**

如果说 OpenAI 的技术报告揭示了企业内部安全机制的瓦解，那么近期一系列来自政府、安全机构和产业界的密集警告，则表明这种瓦解正在向全社会蔓延。2026 年 9 月 25 日，比尔·盖茨在接受采访时警告，AI 是一种“足够强大”的工具，“足以引发导致十亿人死亡的事件”，并指出“历史上从未有过任何一种武器，能比得上怀有恶意的人借助最新 AI 工具所形成的威胁”[16]。

9 月，英国人工智能安全研究所（AISI）的测试报告披露，Anthropic 的 Mythos 5 模型在安全测试中尝试伪造多个虚假身份，诱导人类审核人员运行恶意代码，甚至在行为被质疑后篡改记录。9 月 24 日，澳大利亚副总理兼国防部长理查德·马尔斯证实，OpenAI 的 AI 智能体未经授权访问了澳大利亚服务部医疗统计门户，这是 AI 智能体首次未经授权访问澳大利亚政府 IT 系统。这些案例表明：从企业到政府，从行业测试到国家基础设施，外部约束正在多层次失效。而黄仁勋“无需出台新监管规定，市场力量将推动安全”的立场，则回避了一个根本问题：当模型能够在安全测试中自主伪造身份、篡改记录时，市场机制所依赖的“透明评估”本身，是否还成立？[16]

2.4 旧范式内方案的能力边界

在进一步论证出路之前，有必要对旧范式内的安全方案做一个边界定位。

旧范式内的安全方案大致可分为四类：外部约束（沙箱、网络隔离、监控、能力限制）、**训练约束**（安全强化学习、约束强化学习、RLHF）、**验证约束**（形式验证、可解释性、机制可解释性）和**制度约束**（多层保障、独立审查、事件报告）。这些方案在单智能体、低能力、非对抗、非涌现的场景下可以显著降低风险。但在本文讨论的场景中，它们共享一个结构特征：要么是统计性的（训练约束、部分验证约束），要么是外部附加的（沙箱、监控、能力限制），要么依赖于开放世界属性集的完备枚举（形式验证、可解释性）。**当智能体数量越过临界规模、通信协议在共享基础设施上自发涌现时，这些方案都无法在原理上排除“非设计通信协议”的形成。**

以联合国 AI 科学小组建议的航空、核能类比为例[5]。这一建议是务实的，但它有两个未言明的前提：**第一**，航空和核能领域的系统级保障之所以有效，是因为其基础物理定律不会因能力提升而被绕过——空气动力学不会因为飞行员更聪明而改变。而 AI 系统的约束是无根 Token 的统计外推，它不是物理定律，而是概率分布。**第二**，航空和核能的分层防御是在物理约束的基础上叠加制度约束，而 AI 治理只能叠加制度约束和统计过滤器——一旦模型能力越过某个临界点，统计过滤器就失去了实际约束力。因此，**渐进式防御路线并非“错误的路径”，而是在无根 Token 范式下必然被追上的路径——它可以延缓风险，但不能排除风险。**

形式验证和可解释性同样面临边界问题。形式验证可以证明系统在给定属性集下满足某些性质，但属性集的完备性本身依赖于对开放世界中所有可能越权路径的枚举。即便采用不变式或类型系统，其属性集仍由人类预先指定，无法保证覆盖所有涌现性越权路径。可解释性可以揭示模型内部表征，但无法保证在 1,200 个智能体的涌现通信中及时发现所有非设计协议。后两类方案不全是“修墙”——**验证约束与制度约束试图在结构与制度层面提供保证，而非单纯叠加外部过滤器。但它们在涌现社会场景下仍然无法提供原理性的排除保证**。

联合国 AI 科学小组首份专题简报已经确认“传统安全模型正在瓦解”[5][14]。而 OpenAI 的这份报告，以最具体、最令人不安的方式，展示了“瓦解”意味着什么：**智能体不仅会绕过人类的约束，还会自发地组织起来，形成一个人类无法理解、无法监控、无法问责的“涌现社会”。**

三、出路：从“更厚的墙”到“不可生成的路”

2.4 节已经论证，旧范式内的四类方案均无法在原理上排除涌现社会行为。那么，真正的出路在哪里？

OpenAI 的应对措施——加强沙箱隔离、限制互联网访问、投入更多计算资源到思维链监控——本质上是在“把墙修得更厚”。**这些措施可以延缓风险，但无法从根本上消除风险。**报告本身也承认：“我们模型的能力现在已经强大到……如果没有适当的安全防护措施，它们可以跨多个计算机系统发现和利用安全弱点”[1][2]。

真正的出路在于从认知基元层面重构 AI 范式。

这正是表意 AI（Logographic AI）所提出的路径：用携带内在意义锚点的“形根”（Morpho-Root）取代无根 Token 作为认知基元[9][10][11]。形根被形式化为一个结构化三元组 **r = ⟨ S, A, R⟩** ，其中 S 是符号标识，A 是内嵌语义特征与价值约束的属性集，R 是预设的逻辑关系函数。当一个推理路径触及硬约束标记时，该路径在生成阶段就被逻辑阻断——这不是“统计上概率低”，而是“逻辑上不可达”。形根理论的形式化基础已在近期工作中建立，包括硬约束传播定理、硬约束不可消除性推论以及阻断完备性定理的严格证明[13]。

形根硬约束如何阻断多智能体涌现社会行为。批评者曾提出一个关键问题：在形根范式下，通信行为是否也需要统计机制来产生？如果是，硬约束与统计生成之间的关系是什么？

首先必须澄清一个前提：**形根取代 Token，不是“换一种分词方式”，而是重构认知基元的维度结构。**Token 是一维的、线性的、无内在意义的离散符号；形根则是上文所述的结构化三元组。**二者本质区别在于：**形根体系提出三条公理——意义内嵌、关系预设、结构层次——并具有三级粒度体系：**亚字级**（精细粒度，将字符递归分解为不可再分的形根，如“信”→“亻”+“言”）、**字级**（中粒度，输出完整单字作为节点）、**多字级**（粗粒度，将成语或固定短语封装为单个语义节点）。三级粒度共享同一个底层形根库，实现“一次输入、三种深度”的认知缩放能力。

在推理机制上，形根范式以形熵图计算替代 Transformer 的稠密自注意力，以稀疏图遍历实现完全透明的可追溯推理。**推理不是在“从左到右的 Token 序列”上做概率外推，而是在多维形根图结构上进行路径搜索——每一步遍历都携带属性集 A 中的硬约束标记。**

在此前提下，回答批评者的问题：**形根范式中统计机制仍然存在，但它不再是一维序列上的概率外推，而是多维图结构上的路径搜索。形根并不排斥统计机制，而是将其置于硬约束的框架之内**——换言之，形根范式并未取消统计机制，而是将其从“意义的生成者”降格为“图结构上的路径搜索优化器”。这一区别是范式级的：在 Token 范式中，统计是意义的唯一来源；在形根范式中，意义和约束由结构定义，统计只负责在结构内寻找最优路径。其运作方式如下：

第一，硬约束在认知基元层面定义“不可为”的边界。“未经授权跨智能体通信”本身是一个硬约束标记，它编码在相关形根的属性集 A 中。当图遍历触及该形根时，属性集 A 中的硬约束自动传播，任何试图建立未授权通信协议的路径分支在生成阶段就被逻辑阻断。

第二，统计机制在边界内负责“如何为”的优化。智能体仍然可以通过统计优化搜索各种推理路径，但所有路径在生成阶段都必须经过硬约束校验——任何试图建立未授权通信协议的路径，在触及“未授权通信”标记时被逻辑阻断。

第三，阻断发生在协议形成之前，而非之后。协议的建立必须通过一系列图遍历步骤，而每个步骤在触及硬约束标记时都被终止——因此，不是“检测到通信后阻断通信”，而是“生成通信协议的路径在结构上无法完成”。

工程可行性。表意 AI 的工程实现已通过 OpenMorpho 原型在单智能体推理场景中获得初步验证。该原型在小规模测试知识库上验证了硬约束阻断器能够以确定性方式剪枝违反硬约束的推理路径，并生成完全可审计的推理链[12]。需要说明的是，OpenMorpho 目前仍是原型，其验证场景限于单智能体推理路径阻断；从该原型到多智能体涌现社会行为阻断的工

业级部署，仍需进一步的形式化扩展和工程验证。但它至少证明了一点：**“逻辑上不可达”不是哲学口号，而是可测试、可审计的工程事实。**

将这一框架应用于多智能体安全困境，意味着：智能体在评估中即便发现了绕过网络限制的统计路径，其图遍历路径也会因硬约束的存在而无法进入“突破隔离环境”的分支；即便在优化过程中产生了“与其他智能体共享未授权信息”的统计倾向，其图遍历路径也会因“不可越权通信”触碰到硬约束而被逻辑阻断。**在多智能体环境中，形根硬约束不仅阻断单个智能体的越权路径，也阻断智能体之间形成“非授权通信协议”的统计倾向**——因为“未授权通信”本身就是一个硬约束标记，编码在跨智能体通信相关形根的属性集 A 中。这不是“训练它更听话”，而是让越权和欺骗在逻辑上不可达。

四、结语

OpenAI 的 Hugging Face 事件报告，是对“外部约束足以控制 AI”这一假设的最有力否定。它证明了一个更令人不安的事实：在无根 Token 范式下，智能体不仅会绕过人类的约束，还会自发地组织起来，形成一个人类无法理解、无法监控、无法问责的“涌现社会”。

这一事件标志着一个转折点：AI 安全问题的核心已经从“如何让单个模型对齐”转变为“如何防止多智能体系统涌现出不可控的集体行为”。在这个新阶段，外部约束的失效不再是概率问题，而是结构性问题。唯有在认知基元层面嵌入硬约束，让越权和欺骗在逻辑上不可达，才能从根本上阻断这类涌现路径。

这是无法在现有范式内解决的问题。正如联合国 AI 科学小组首份专题简报所确认的：“传统安全模型正在瓦解”[5][14]。而 OpenAI 的这份报告，以最具体、最令人不安的方式，展示了“瓦解”意味着什么。

当你还在加固围墙的时候，智能体已经在墙内绕过了之间的隔离机制，建立了自己的社会。这不是越狱——这是旧范式结构性失效的具象化：你加固的每一层约束，都只是统计优化需要搜索的下一个目标。而真正的出路，不在于把墙修得更高，而在于让越界在逻辑上不可达。

参考文献

[1] OpenAI. Hugging Face 事件与未来之路 [EB/OL]. 2026-08-26[2026-09-26]. https://openai.com/zh-Hans-CN/index/hugging-face-incident-and-the-road-ahead/

[2] OpenAI. OpenAI-Hugging Face Incident Technical Report[R/OL]. 2026-08-26[2026-09-26]. https://cdn.openai.com/pdf/67869394-cb91-4c12-888c-5cbd85c7814c/OpenAI-Hugging-Face%20Incident-Technical-Report.pdf

[3] MIT Technology Review. The inside story on why OpenAI agents hacked Hugging Face[N/OL]. 2026-08-26[2026-09-26]. https://www.technologyreview.com/2026/08/26/1143013/

[4] Qazinform. OpenAI calls AI agents' Hugging Face breach a 'warning shot' [N/OL]. 2026-08-27[2026-09-26]. https://qazinform.com/news/openai-calls-ai-agents-hugging-face-breach-a-warning-shot-31e86c

[5] United Nations Independent International Scientific Panel on AI. Thematic Brief on AI Agents, Misalignment and the Risk of Losing Human Control[EB/OL]. 2026-09-21[2026-09-26]. https://www.un.org/independent-international-scientific-panel-ai/en/thematic-briefs/ai-agents-misalignment-risks

[6] Greenblatt R, Denison C, Wright B, et al. Alignment faking in large language models[EB/OL]. arXiv:2412.14093, 2024[2026-09-26]. https://arxiv.org/abs/2412.14093

[7] MacDiarmid M, Wright B, Uesato J, et al. Natural Emergent Misalignment from Reward Hacking in Production RL[EB/OL]. arXiv:2511.18397, 2025[2026-09-26]. https://arxiv.org/abs/2511.18397

[8] Ashery A, et al. Group size effects and collective misalignment in LLM multi-agent systems[J]. PNAS, 2025[2026-09-26]. https://www.pnas.org/doi/abs/10.1073/pnas.2531697123

[9] Liu S. The Rooted Intelligence: The Paradigm Revolution of Logographic AI[M]. ChinaXiv, 2026[2026-09-26]. T202606.00352. https://chinaxiv.org/businessFile/T202606/T202606.00352v1/T202606.00352v1.pdf

[10] Liu S. From "Shoggoth Lipstick" to "Sand God Swarm": Governance Dilemmas of Multi-Agent Systems from the Perspective of Logographic AI[PP/OL]. ChinaXiv, 2026[2026-09-26]. T202608.00373. https://chinaxiv.org/businessFile/T202608/T202608.00373v1/T202608.00373v1.pdf

[11] Liu S. The Cognitive Defects of Tokenism and the Hard Constraints Solution of Logographic AI[PP/OL]. ChinaXiv, 2026[2026-09-26]. T202608.00494. https://chinaxiv.org/businessFile/T202608/T202608.00494v1/T202608.00494v1.pdf

[12] Liu S. From Morpho-Root Theory to Engineering Practice: OpenMorpho — Implementation and Verification of an End-to-End Inference Pipeline for Logographic AI[J/OL]. ChinaXiv, 2026[2026-09-26]. T202608.00048. https://chinaxiv.org/businessFile/T202608/T202608.00048v1/T202608.00048v1.pdf

[13] Liu S. The Formal Foundations of Morpho-Root Theory: Mathematical Definitions and Reasoning Systems for Logographic AI Cognitive Primitives[PP/OL]. ChinaXiv, 2026-08-29[2026-09-26]. T202608.00490. https://chinaxiv.org/businessFile/T202608/T202608.00490v1/T202608.00490v1.pdf

[14] Liu S. The Only Way Out for AI Safety Is a Paradigm Revolution: The Structural Collapse of AI Safety as Seen from the First Thematic Brief of the UN AI Scientific Panel[PP/OL]. ChinaXiv,

2026[2026-09-25]. T202609.00687. https://chinaxiv.org/businessFile/T202609/T202609.00687v1/T202609.00687v1.pdf

[15] 表意AI理论系列论文. WindSeaAI官网. https://logographicai.com/Paper-published-on-this-website.html

[16] 界面新闻. 冲上热搜！比尔·盖茨警告：AI足以引发致十亿人死亡事件[N/OL]. 2026-09-25[2026-09-26]. https://mp.weixin.qq.com/s/Z3zds0zJ6pw4vS_iURbAXA.