NETWORLD EUROPE

智能体AI的挑战与应对

Rui L. Aguiar教授

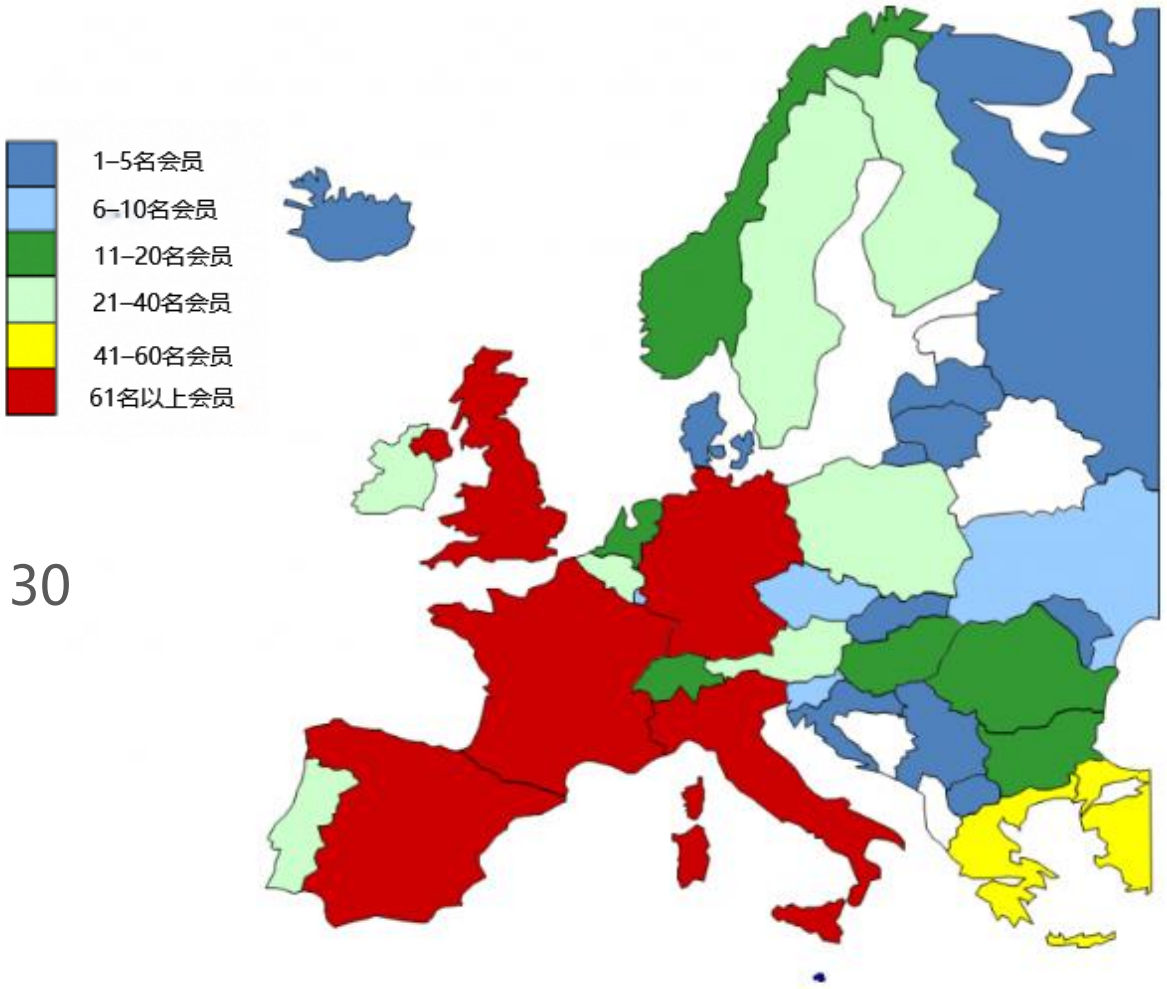
指导委员会主席

目标

- 输出相关技术、研究和社会问题的立场文件。
- 通过与政治和公共领域、业界及学术界的决策者展开对话，弥合研发与欧洲社会期望之间的差距。
- 根据欧盟智能网络和服务联合体（Smart Networks and Services Joint Undertaking，SNS JU）具体的谅解备忘录，定期为欧洲通信网络制定更新的战略研究和创新议程（SRIA）。
- 加强欧洲在网络技术和服务方面的领导地位，使其更好地为欧洲公民和欧洲经济服务。
- 支持5G公共和私人设施合作项目（5G PPP）和SNS JU。

NETWORLDEUROPE会员

- 约1,000名会员
  - 行业单位（大企业）：~150
  - 研究组织：~330
  - 中小企业：~350
  - 合作组织（如欧盟以外的注册实体）：~130



战略研究和创新议程（SRIA）

NetworldEurope 2026年的SRIA将通过以下五个主要路线进行重新设计：

- 系统视图和架构方向
- 网络的软件化和智能化
- 协议和通信范式
- 物理层创新
- 跨领域和颠覆性技术

有几个主题涉及所有领域（例如安全、设备、可持续发展等）。

NETWORLD EUROPE

智能体AI与挑战

基础准备工作
重点工作回顾：智能网络和服务（SNS）与运营商

- HORIZON-JU-SNS-2023-STREAM-B-01-06“欧盟-美国6G 研究和创新合作”：为6G研究中的人工智能/机器学习（AI/ML）集成做好准备工作，包括数据生成、共享数据集和通用评估框架。
- HORIZON-JU-SNS-2024-STREAM-B-01-08“面向6G通信系统和服务的可靠AI”：旨在AI/ML解决方案的端到端系统集成，以及AI原生网络功能的研究。
- （2025年规划，仍未激活）跨Stream B主题的强制性开放AI/ML训练数据发布——数据集创建和共享是2025计划的内置要求。
- （待定）HORIZON-JU-SNS-2026-STREAM-B-01“适用于为6G网络和AIaaS训练AI模型的数据集的收集、生成和验证”：生成精选的数据集合以及支持基础设施，为6G网络和服务开发强大的AI模型。

基础准备工作
重点工作回顾：EU Cluster 4（数字技术领域的战略集群）

- 2025年：Cluster 4数字化征集项目下的若干AI和生成式AI主题（例如，认知计算、AI的软件工程、通用人工智能（GP-AI）战略）
  - HORIZON-CL4-2025-04-DATA-02：通过认知计算连续体增强AI/生成式AI
  - HORIZON-CL4-2025-04-DATA-03：面向AI和生成式AI的软件工程
  - HORIZON-CL4-2025-04-DIGITAL-EMERGING-04：通用AI能力和风险的评估方法
  - HORIZON-CL4-2025-04-DIGITAL-EMERGING-07：通用AI的增强学习策略：推进GenAI4EU
- 2026年：“新兴数字技术”项目面向AI的征集（AI智能体、生成式AI助推器、AI科学试点、机器人平台）
  - HORIZON-CL4-2026-05-DIGITAL-EMERGING-02：面向真实世界应用的下一代AI代理研究与创新行动（Research and Innovation Action，RIA）
  - HORIZON-CL4-2026-05-DIGITAL-EMERGING-03：应用AI：敏捷和智能机器人平台研究与创新行动
  - HORIZON-CL4-2026-04-DIGITAL-EMERGING-19：基于挑战驱动的GenAI4EU助推器在应用AI中的优先落地领域（研究与创新行动）
  - HORIZON-CL4-2026-04-DIGITAL-EMERGING-01：应用AI：欧洲人工智能科学资源（Resource for AI Science in Europe，RAISE）战略项目支柱：“Science for AI”试点

人工智能的演进：从静态模型到推理型代理

传统AI

基于规则和机器学习的模型

- 孤立的、特定领域的任务执行
- 无记忆能力
- 无法进行超出训练数据范围的推理
- 集中控制
- 适应性有限

- 学习能力的挑战
- 质量分类的挑战

生成式AI/LLM

认知自动化

- 自然语言推理、工作流程自动化、意图解析
- 基本上仍是集中式的、静态的工作流程

- 意图解析缺乏保障
- 操作范围有限

智能体AI

自主规划、行动和学习的智能体

- 感知环境
- 分解目标
- 使用工具
- 协作
- 持续和自主地自修复

- 信任与保障
- 循环状态避免
- 大规模一致性

本页材料改编自： Wei et al., "Agentic Reasoning for Large Language Models", arXiv:2601.12538, 2026

智能体AI与其他AI的不同

范式	主要输出	典型的自主程度	在电信领域的应用
基于规则的自动化	确定性行动	低	重复性工作流程
预测型机器学习	预测结果/得分	中	检测 + 优化输入
生成式AI助手（Copilot）	输出解释/制定计划	中	为运营商提供辅助
代理型AI	执行的工作流程 + 结果	高（有边界）	意图到保障；闭环反馈

已非常常见

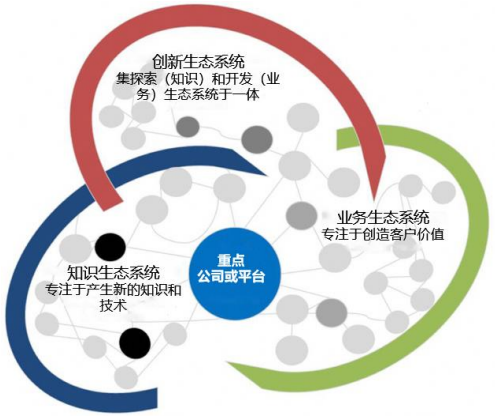
在许多领域都有应用

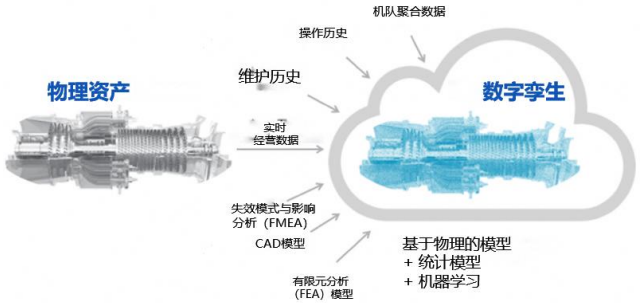
有限使用

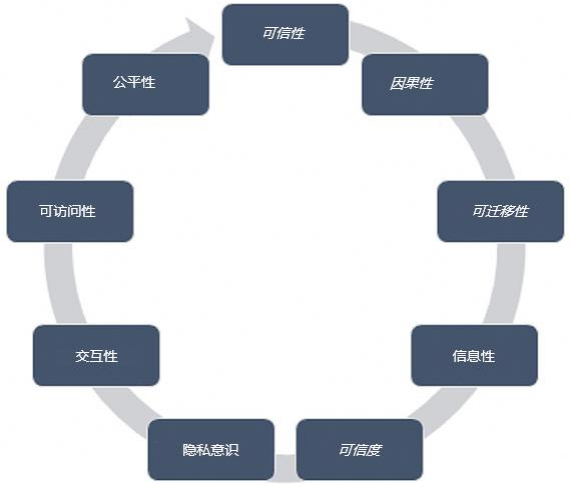
探索阶段

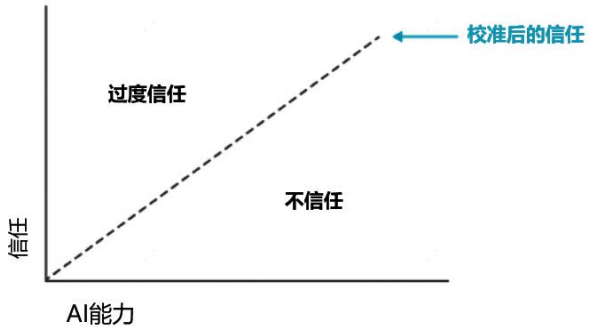
当前需要反思的话题

- 有生态系统与无生态系统的区别
  - 自研解决方案 vs 外部专家知识
  - 混合解决方案
  - 行动的审计和解决方案质量的评估
  - 一刀切的解决方案？AI代理的质量和目标?
- 所需的数字孪生
  - 安全、规划、优化都不可避免地需要数字孪生?
- 对系统的控制和理解
  - 行动的可见性
  - xAI
  - 意图的实现和验证
  - 对代理和解决方案提供商的信任：网络安全
- 大规模互动
  - 已验证的代理 ≠ 已验证的代理系统
  - 所有权 ≠ 责任
- 数据、法律和法规
  - 欧盟《通用数据保护条例》（GPDR）和数据使用
  - 人工智能法案（AI Act）和人类控制（human-in-control）原则
  - 数据所有权和相关性









向新系统演进

- 渐进式应用结合分层方法
  - 顶层：客户相关的操作与辅助式操作、管理和维护（OAM）
    - 非关键性错误/失误/误操作，且可由人类监督
  - 底层：物理层优化
    - 应用范围有限，环境更受控，法律障碍较少
- 数据与标准的平衡
  - 逐步推进的商业化路径
  - 信任与质量问题的构建，随着生态系统的逐步完善，最终形成真正的行业解决方案
    - 运营商 vs 制造商 vs 解决方案提供商
    - 谁将能够训练和交付哪些代理以达到什么目的

当前的危险：在没有经过真正验证的情况下就匆忙推出和采用解决方案，这将危及技术的潜力

NETWORLD EUROPE

感谢聆听

networldeurope.eu