文章类型：论文|刊号（ISSN）：2630-5178 /（中图刊号）：380GL019

T 型人才视角的智能体安全治理课程体系建设

李世颉
中南民族大学
DOI:10.32629/mef.v8i21.18304

[摘　要] 智能体技术的兴起推动了国家安全治理迈入人机共生时代,高校国家安全教育亟需拥抱技术、重塑培养范式。本文基于T型人才视角构建课程体系,以“垂直深耕+水平跨越”弥合技术与治理割裂：既强调“懂技术、会实操”,亦强调“明风险、守底线、知敬畏”。通过“构建-管控-前瞻”闭环教学,培养兼具智能体技术能力与国家安全战略、伦理法治素养的复合型人才,为国家安全体系和能力现代化提供支撑,并为新文科交叉课程改革提供可复制范式。
[关键词] 智能体；国家安全治理；T型人才；课程体系改革
中图分类号：TN915.5　文献标识码：A

Construction of a Curriculum System for Agent Security Governance from the Perspective of T-shaped Talents

Shijie Li
South-Central Minzu University

[Abstract] The rise of AI agents propels national security governance into human-machine symbiosis, necessitating universities to reshape talent cultivation paradigms. Based on the "T-shaped Talent" perspective, this paper constructs a curriculum system using a "vertical deepening + horizontal spanning" approach to bridge the technology-governance divide. It balances technical proficiency with risk awareness and ethical reverence. Through a "construction-control-foresight" closed-loop model, the system cultivates composite talents combining AI agent capabilities with strategic and legal literacy. This work supports national security modernization and offers a replicable paradigm for "New Liberal Arts" reform.
[Key words] AI Agents; National Security Governance; T-shaped Talent; Curriculum System Reform

引言

当前,AI正经历从感知向认知、从专用向通用智能的跨越,依据智谱AI对AGI发展阶段的分类,当AGI演进至L3时,系统不再是单纯信息处理工具,而是进化为具备主动感知、自主规划、工具调用及自我反思能力的“智能体”。产业层面,面向智能体的开源编排框架(如CrewAI)与国内企业级产品(如“实在Agent”、“OmBot”)加速涌现,反映出智能体正从研究原型迈向规模化探索。在此背景下,国家安全治理面临双重挑战：一方面,智能体是提升情报搜集、舆情研判及设施防护效率的关键“利器”；另一方面,其自主决策不确定性、算法黑箱不可解释性及被恶意利用风险,使其成为必须时刻防范的“对象”。这种“工具-对象”二元同构,要求治理必须从“被动防御”转向“主动治理”,从“人力密集”转向“人机协同”。然而,审视当前高校国家安全教育,普遍存在人才能力结构失衡的问题,表现为“深井”与“孤岛”效应：一方面,理工科学生深陷技术细节“深井”,精通算法代码,但缺乏国家安全战略宏观认知,难以理解技术背后的政治、社会与法律边界,易导致“技术至上”的伦理失范；另一方面,文科(如国关、公管)学生虽具战略思维,但缺乏前沿技术“深潜”能力,对AI Agent理解停留在概念层面,无法掌握其运行逻辑,这种技术认知“孤岛”使其面对深度伪造、自动化网络攻击等新型威胁时,难以提出切实可行方案。为破解这一困局,引入“T型人才”范式尤为迫切,根据印第安纳大学CITL定义,“T型学生”由代表深厚学科知识的垂直维度与代表跨越边界核心素养的水平维度组成。在智能体治理语境下,该范式具有极高适切性：垂直维度要求打破计算机与国安学科壁垒,形成“技术+业务”双重深度；水平维度要求具备批判性思维、伦理判断与跨域协作能力,以应对AGI时代复杂挑战。本研究旨在基于此范式,构建人才能力结构模型并设计课程映射方案,且研究建立在扎实教改实践基础之上。研究对象——智能体安全治理课程体系,依托已获批的《智能体(AI agents)技术在国家安全治理中的应用与管理》教改项目,该体系于2025年在中南民族大学国家安全学院建立并面向研究生开设。实践中,团队紧密结合边疆社会文

化安全与口岸要地安全治理需求,引入CrewAI、LangChain等框架,开展自主情报搜集、认知对抗及基建保护等多项实战教学。本研究即对该体系从设计到实施的系统总结,旨在为新文科交叉课程建设提供可复制范本。

图1 面向智能体安全治理的“T型”人才能力结构模型

1 垂直维度：学科专业知识“深潜”与重构

在T型模型中,垂直维度是立身之本。对本课程体系而言,垂直维度非简单“技术扫盲”,而是将“AI前沿技术”与“国安实战业务”深度熔炼,形成核心竞争力。课程通过三大模块深耕,重构学生知识体系。

1.1技术架构深度:从原理到部署的底层穿透。治理智能体,必先理解智能体。不同于传统AI课程侧重模型训练,本课程垂直深度首先体现在解构AI Agent架构。课程要求深入掌握“AI Agent=LLM(大脑)+Planning(规划)+Memory(记忆)+Tools(工具)”范式。学生不仅要理解LLM如何作为认知核心,更要探究智能体如何通过思维链拆解任务,如何利用向量数据库实现记忆,及如何调用API改变物理或数字世界。这种原子层面“深潜”,是识别系统脆弱性、设计防御策略的逻辑起点。

图2 智能体安全治理课程体系内容的“技术-业务”映射图

1.2业务场景深度:三大实战领域垂直深耕。立足边疆社会文化与口岸要地安全,课程在垂直维度构建三个高精度实战场景,要求学生达到“准专家”深度。

1.2.1自主情报搜集深耕。针对开源情报海量、异构、动态特点,课程不满足于传统搜索技巧,而深入智能体构建。深度要求上,学生需掌握利用CrewAI等框架设计“Agent团队”。技术业务融合上,要求深入学习多源融合技术,实现对全球网络、社媒及暗网全天候监测;掌握利用智能体自动识别恐怖组织与极端主义动向。这使学生具备利用AI重塑情报生产流程的实战能力。

1.2.2信息战与认知对抗深耕。面对虚假信息与深度伪造泛滥,课程聚焦对抗智能体开发。深度要求上,学生需探究深度伪造原理与检测算法,掌握基于Transformer的文本分类模型训练。技术业务融合上,构建能实时监测舆情智能系统,精准标记虚假宣传,并在伦理允许范围内,设计能生成正面叙事并自动传播的对抗性智能体。这要求建立算法与传播学的深度连接。

1.2.3基础设施防护深耕。针对边疆口岸及要地,课程聚焦基建保护与应急响应智能体。深度要求上,强调复杂系统风险建模,掌握动态压力测试脚本编写。技术业务融合上,构建全维感知安防智能体,集成云网边端数五大要素。学生需设计能自主评估风险、异常检测并触发应急响应(如切断网络、锁定门禁)的决策系统。通过深耕,学生不再是理论家,而是具备特定场景解决问题能力的技术专家。

2 水平维度：跨界核心素养“广延”与培育

垂直维度决定“硬实力”,水平维度决定“软实力”。依据IU定义,水平维度强调“边界跨越”。课程通过教学设计,培育学生跨越学科、伦理、人机及国界四大边界素养。

2.1跨越思维边界:批判性思维与复杂系统认知。智能体增加治理复杂性,水平维度的首要任务是培养批判性思维。一是风险审视,课程设置《智能体技术风险挑战》模块,引导学生跳出技术乐观陷阱,审视脆弱性。例如,探讨“智能体被恶意提示攻击时,如何防其成为工具?”二是系统观,培养全生命周期视角。不仅关注部署效能,更关注设计合规、运维治理及退役风险。这种思维使学生能跨越单点,洞察治理生态关联。

2.2跨越价值边界:伦理判断与社会责任。技术中性,使用有导向。T型人才需具备伦理素养。一方面,课程将“发展与安全并重”贯穿始终,在《伦理原则》一章中深入探讨算法偏见、隐私侵犯及“信息茧房”,倡导科技向善。另一方面,引导思考责任归属,如“自主智能体决策失误(如误判情报)时,责任在开发者、部署者还是AI?”通过思辨,让学生内化“科技向善”准则,确保技术实践坚守底线。

2.3跨越协作边界:人机协同与多主体共治。AGI治理是人机协同(Human-AI Teaming)复杂博弈。水平维度重点培养协作力。人机协作层面,通过多智能体实验,让学生体验作为“指挥官”与“AI下属”的分工,理解“人在回路”保障决策安全的重要性。跨部门协同层面,探讨军民融合、央地协同及数据共享,培养学生面对跨域威胁时,打破壁垒调动资源协同治理的能力。

2.4跨越地缘边界:全球视野与法治精神。治理具有国际性,水平维度强调视野拓展。一是比较视野,对比美欧中战略差异,引导学生理解地缘政治下的治理逻辑,培养其参与国际规则制定的能力。二是法治思维,在《法律制度适应性改革》一章中探讨现行法律对智能体责任界定的适用性,培养法治轨道推进创新的精神。

文章类型：论文|刊号（ISSN）：2630-5178 /（中图刊号）：380GL019

3 整合机制：基于“构建-管控-前瞻”的项目式熔炉

T型人才垂直与水平维度需有机融合。课程提出“构建-管控-前瞻”三位一体整合机制，通过项目式学习映射教学流程。

图3 “构建-管控-前瞻”项目式教学闭环流程图

3.1构建(Build)：场景驱动技术实战。作为垂直维度载体，依托16学时《应用实践》与14学时《实验》。过程循序渐进：首先OSINT智能体搭建，学生利用LangChain/CrewAI写代码，从零构建情报系统；其次虚假信息检测，利用Scikit-learn处理数据集训练模型；最后基建风险建模，对数据中心仿真。此环节通过高强度实践，夯实“垂直深度”。

3.2管控(Control)：全生命周期风险复盘。此机制对应水平维度批判思维与伦理，将《管理治理》嵌入实战，强制“技术与风控并行”。构建时必须同步完成全生命周期管理计划。如设计OSINT时界定采集边界；训练时检测数据偏见。此外，要求提交《风险识别评估与管控报告》，运用模型(如风险矩阵)对系统全面“体检”。这迫使学生写代码时思考后果，实现技术与治理思维融合。

3.3前瞻(Think)：战略高度博弈演练。为提升全球视野，课程通过《前沿发展》与大作业升华。组织红蓝对抗，一组利用AI生成虚假信息(红队)，一组识别反制(蓝队)。演练后复盘，探讨“认知战对政权安全长远影响”。同时要求结合AGI L3趋势撰写论文(如《AGI时代治理变革》)，引导跳出细节，从现代化高度思考法律规制与博弈策略。

4 结语

智能体技术开启了国家安全治理的人机共生新纪元，高校亟需重塑人才培养范式。本研究提出基于“T型人才”视角的课程体系，通过深耕技术与跨越治理，解决了传统教育中两者割裂的难题。该体系强调技术实操与风险伦理并重，采用“构建-管控-前瞻”闭环教学，旨在培养驾驭前沿技术且深谙战略法治的复合型人才。此改革为国家安全现代化提供了人才支撑，也为新文科背景下的交叉学科改革提供了推广范式。

本研究得到中南民族大学校级教学改革项目《人工智能与政府绩效评价》资助(项目编号：JYX20042)。

[参考文献]

[1]Gartner. Top 10 Strategic Technology Trends for 2025 [EB/OL].2024-10-21.

[2]Gartner. Predicts Over 40% of Agentic AI Projects Will Be Canceled[EB/OL].2025-06-25.

[3]Spataro J. New autonomous agents scale your team like never before[EB/OL].Microsoft,2024-10-21.

[4]Salesforce. Agentforce Is Here: Trusted, Autonomous AI Agents[EB/OL].2024-10-29.

作者简介：

李世颉(1983--),男,回族,湖北省武汉人,博士,副教授,研究方向：人工智能教育,电子政务。