

美国国防情报局人工智能主管展望支持军事行动的“智能体对智能体”交互

来源: 美国 Defensescoop 网站 发布时间: 2026/08/13

基本信息

关键词	美国国防情报局, 人工智能, 军事行动, 智能体
来源	美国 Defensescoop 网站
发布时间	2026/08/13
原文链接	https://defensescoop.com/2026/08/13/dia-artificial-intelligence-agent-to-agents/

具体内容

美国国防情报局 (DIA) 的首席人工智能官正在展望一个未来: 数字智能体在作战司令部范围内协同工作, 帮助军队和情报界完成任务。

金尼少将 (Maj. Gen. Robert Kinney) 周三在佛罗里达州坦帕市举行的“国防部情报信息系统” (DODIIS) 全球会议上参加小组讨论时表示, DIA 目前正在开展一项为期 90 天的“冲刺”计划, 以构建一个人工智能企业平台服务。

他指出, 另一个正在推进的“交付成果”是模型上下文协议 (Model Context Protocol, 简称 MCP), 它将提供一种“更通用的方式”来访问情报数据。

MCP 是一种允许人工智能工具与外部系统和数据源连接的技术框架。

金尼说: “不过, 在此基础上——我估计, 我不会过度承诺或交付不足——但在未来一年的规划中, 构建智能体, 然后是‘智能体对智能体’ (agents-with-agents), 是我们想要前进的方向。在合规性、安全性、零信任方面, 还有一整套其他工作, 我们将与首席信息官

(CIO) 的同事们合作推进。”

在展望未来的两到五年时，他表示重点将放在 MCP 和人工智能“智能体对智能体”的交互能力上。

“想象一下，在作战司令部里，一个负责收集管理的智能体正在与负责作战（3 号局）的智能体对话，并可能与负责火力（fires）的智能体交流，与负责对抗性后勤（4 号局）的智能体对话，与负责指挥、控制、通信和网络（6 号局）或负责规划（5 号局）的另一个智能体对话。这就是未来的方向。”金尼描述道。

然而，官员们需要考虑如何最好地建立护栏，以降低与该技术潜在输出相关的风险。他指出，一个关键的考量因素是，在某些情况下，这些能力的潜在效果是可逆的还是不可逆的。

“我认为，当然存在一些任务领域……可以接受更高的风险，并采用‘人在回路监控’（human on the loop）模式，而不是‘人在回路控制’（human in the loop）模式。但对于那些更不可逆的任务领域——比如你们可以想到的火力打击等——随着能力的不断提升，必须始终有‘人在回路控制’。这必须作为一个智能体检查环节存在。”金尼说。

DIA 目前正在努力铺设支持数据访问和构建新智能体的数字基础和“管道”。

金尼表示，官员们还在思考“相关的技术手段，以及如何负责任地使用智能体之间的交互，不过度依赖这项技术，并在一套特定的参数范围内运行。”