微软与诺基亚携手探索“AI 自主防御”：电信运营商网络安全进入智能体时代

在过去几年里，全球电信行业一直在讨论“自智网络（Autonomous Networks）”的未来。随着 5G、云原生架构、生成式 AI 以及网络自动化技术不断成熟，运营商希望网络能够像“自动驾驶”一样，实现自配置、自优化、自修复，甚至自主决策。但当网络越来越智能，一个新的问题也随之浮现：当攻击者同样开始使用 AI，未来的通信网络究竟该如何防御？

近日，Nokia 与 Microsoft 联合发布了一份关于 AI 安全的重要行业白皮书——《Securing autonomous telecom networks with AI-driven defense》。相比传统意义上的网络安全报告，这份文件更像是一份关于未来运营商网络形态的预判。它不仅讨论了 AI 时代的安全风险，更提出了一个正在被行业广泛接受的新观点：

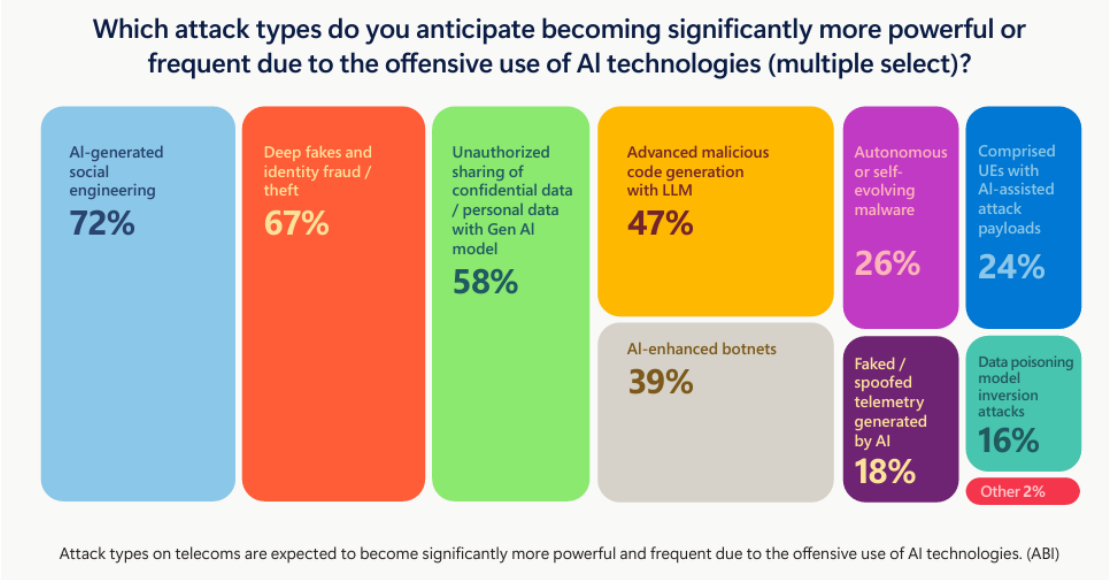
未来的电信网络，必须依靠 AI 来保护 AI。

AI 正在改变运营商网络的“攻击逻辑”

对于运营商而言，过去十年最重要的变化，是网络从封闭、专有架构逐渐走向开放、云化和软件化。尤其是在 5G 时代，大量网络功能开始运行在云平台之上，OSS/BSS 系统持续自动化，边缘计算节点快速增加，网络与 AI 系统之间的耦合也越来越深。这种变化极大提升了运营效率，但也让网络攻击面急剧扩大。

白皮书指出，当前运营商面临的威胁已经不再是传统意义上的恶意代码或单点攻击，而是进入了“对抗性 AI（Adversarial AI）”阶段。攻击者开始利用生成式 AI 批量生成恶意代码，通过大语言模型发起更复杂的社会工程攻击，甚至利用 Deepfake 进行身份伪造。与此同时，AI 增强型 Botnet、自主进化恶意软件以及伪造遥测数据等新型攻击方式，也开始逐渐出现。

根据报告引用的 ABI Research 数据，超过七成运营商认为，AI 生成的社会工程攻击将在未来显著增加，而深度伪造和身份欺诈则成为行业最担忧的风险之一。



对于运营商而言，这意味着一个根本性的变化：网络安全已经不再是“防火墙+规则库”的传统模式，而正在演变为一场 AI 与 AI 之间的对抗。

运营商开始意识到：传统 SOC 已经跟不上 AI 攻击速度

在传统安全体系下，大多数运营商仍然依赖 SOC 团队进行告警分析、事件关联和人工处置。但问题在于，AI 时代的攻击速度已经远超人工响应能力。

微软与诺基亚在报告中提到，如今的威胁不仅数量庞大，而且具备高度动态化和持续演化特征。攻击行为可能在几分钟内快速扩散，而传统人工分析往往需要数小时甚至数天。也正因为如此，“Agentic AI（智能体 AI）”开始成为这份白皮书的核心关键词。

与传统自动化不同，Agentic AI 并不仅仅执行预设脚本，而是具备一定程度的自主推理与行动能力。它能够持续监测网络环境，自主发现异常行为，并根据上下文动态调整防御策略。报告中特别提到，诺基亚正在将 Agentic AI 引入其 NetGuard 安全体系之中。这些 AI Agent 能够完成完整的威胁狩猎流程，包括：

- 自动生成检测假设
- 动态构建规则
- 分析攻击路径
- 关联多域告警

- 执行威胁遏制
- 自动生成报告

过去需要 SOC 团队耗费数小时完成的工作，现在可能在几分钟内完成。而这也意味着，运营商安全团队的角色正在发生变化。过去，安全工程师更多承担“执行者”的角色；而在未来，他们将更像是 AI 系统的“监督者”和“决策者”。

AI 安全不再只是“防御成本”，而是运营商的新增长能力

值得注意的是，这份报告并没有把 AI 安全仅仅定义为“风险管理”。相反，微软与诺基亚反复强调：AI 驱动的自智网络，本质上正在成为运营商提升业务竞争力的重要基础设施。

白皮书中引用的多项行业数据显示，自智网络已经开始带来可量化的商业收益。例如：

- 网络运营效率平均提升约 20%
- OPEX 下降约 18%
- 超过 70%的运营商实现能耗优化
- Autonomous Network 项目 ROI 可达到 1.7 倍至 3.4 倍

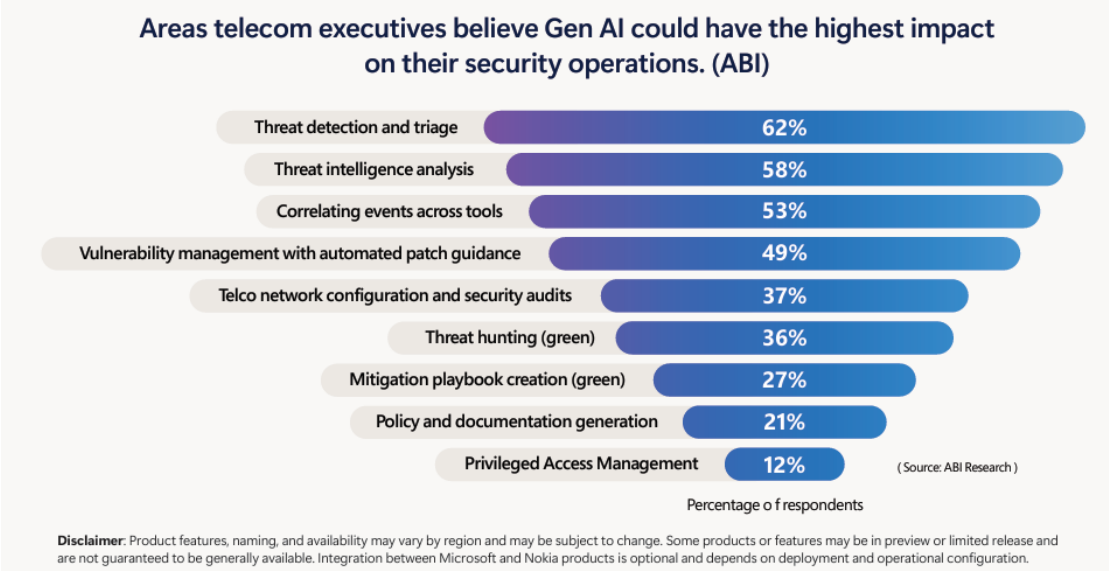
这些数字背后，其实反映的是运营商商业模式的一次深层变化。长期以来，通信行业始终面临“增量不增收”的压力。传统流量业务增长放缓，但网络复杂度却持续上升，运营成本不断增加。而 AI 驱动的自智网络，则让运营商第一次有机会真正实现：

“网络越复杂，运营成本反而越低”。

与此同时，更智能的网络调度能力，也意味着更稳定的 QoS、更低的时延和更快的问题恢复能力。这些能力最终会直接影响：

- 用户满意度
- 客户留存率
- 高价值业务承载能力
- 企业专网体验
- ARPU 增长

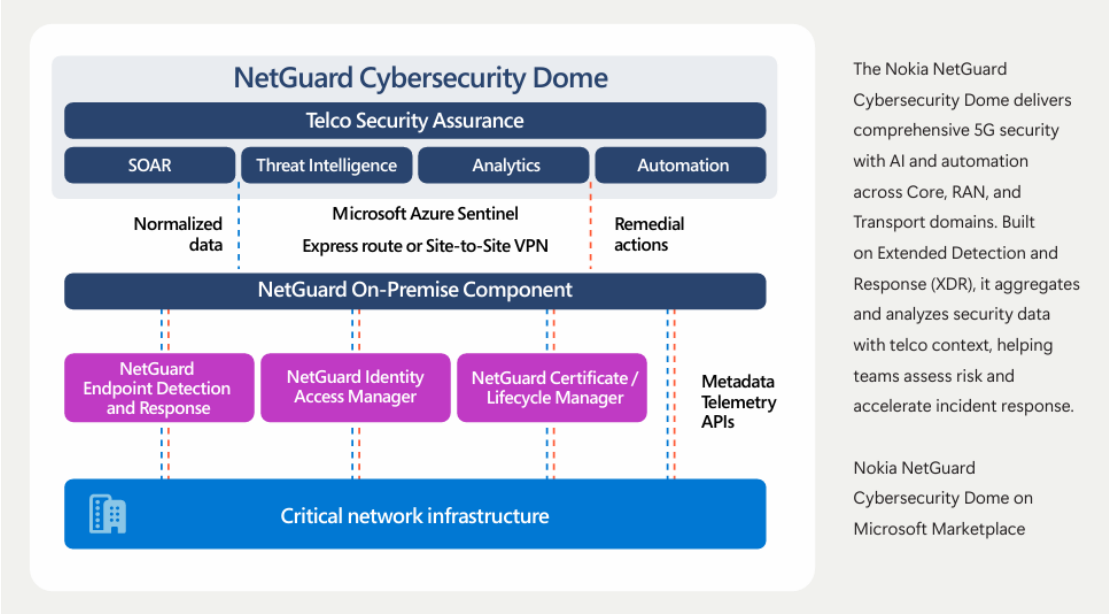
从这个角度看，AI 安全已经不仅仅是技术问题，而正在成为运营商未来收入增长模型的重要组成部分。



诺基亚与微软：面向自智网络的 AI 原生安全体系

为应对这一趋势，诺基亚与微软深度协同，推出面向自智网络的一体化安全解决方案，将微软的云能力、生成式 AI 与零信任架构，与诺基亚的电信级网络安全、智能体 AI 及全域威胁运营能力进行深度融合，形成覆盖网络、云、边缘、终端与数据的全方位防御体系。在方案底座层面，微软提供 Azure Operator Nexus、Microsoft Fabric、Azure Sentinel、Security Copilot、Azure OpenAI 等核心能力，构建安全、合规、可扩展的云平台，支持网络遥测数据实时处理、AI 模型规模化部署、安全事件智能分析与自动处置，并通过 Microsoft Purview 实现策略自动化、审计可追溯与数据安全治理，确保自智网络在全生命周期内满足严格合规要求。

在电信网络安全侧，诺基亚以 NetGuard Cybersecurity Dome（XDR）平台为核心，打造面向通信场景的扩展检测与响应能力，覆盖核心网、无线接入网、传输网、边缘节点等全网络域，可在异构设备与多厂商环境中完成告警归一、智能关联、威胁降噪与上下文分析，将威胁检测时间缩短 40%。更为关键的是，方案融入诺基亚自研的电信专用大模型与智能体 AI（Agentic AI），通过持续自主威胁狩猎、动态更新检测规则、自动化处置流程，将传统依赖人工分析的威胁驻留时间从“天级”压缩至“分钟级”，并将安全分析师日常工作量降低 60%，为自智网络实现“感知 - 分析 - 行动”闭环自智提供核心引擎。



在实际部署中，诺基亚 NetGuard XDR 与微软 Azure Sentinel 通过专线或 VPN 实现深度对接，打通网络侧与云侧安全数据，形成“网络纵深防御 + 云规模智能分析”的协同格局。这一联合方案不仅能够有效抵御 AI 驱动的复杂攻击、应对日益复杂的合规压力，还能支撑自智网络从 L0 人工运维向 L5 完全自智的平滑演进，在提升运营效率、降低能耗与成本的同时，为下一代通信基础设施构建高韧性、高可靠、高安全的技术底座。

云原生，成为自智网络时代的底层基座

在这份报告中，微软与诺基亚还释放了另一个非常明确的行业信号：未来自智网络的核心基础，不再是传统封闭式设备，而是云平台。报告指出，许多运营商过去对于 SaaS 和公有云始终保持谨慎，尤其担心数据主权、合规和关键网络控制权问题。

但随着 AI 能力越来越依赖超大规模算力与实时数据分析，运营商已经很难继续依靠传统本地化架构支撑未来网络演进。因此，微软与诺基亚正在尝试构建一种“安全云+AI 自智”的联合架构。其中包括：

- Microsoft Azure
- Azure OpenAI
- Microsoft Sentinel
- Security Copilot
- Azure Operator Nexus

以及诺基亚的：

- NetGuard XDR
- NetGuard Cybersecurity Dome
- Predictive Security Framework

通过统一云平台、遥测系统和 AI 分析能力，实现跨域网络安全协同。在这种架构

下，网络将逐渐具备真正意义上的：

- Self-Healing（自愈）
- Self-Optimization（自优化）
- Intent-based Automation（意图驱动自动化）
- Closed-loop Operations（闭环运营）

这也被认为是迈向 L4/L5 级自智网络的关键一步。

电信行业的竞争，正在从“连接能力”转向“AI 运营能力”

事实上，从整个行业趋势来看，这份白皮书背后真正值得关注的，并不是某一个安全产品，而是运营商竞争逻辑的变化。过去，通信行业的核心竞争力主要来自：

- 频谱资源
- 网络覆盖
- 基站规模
- 带宽能力

但未来，运营商之间更重要的竞争，可能会变成：谁更早拥有 AI 驱动、自主运行、自主防御的智能网络体系。因为在 AI 时代，网络已经不再只是“传输通道”，而开始演变成一个具备实时感知、自主决策和动态优化能力的智能系统。而 Agentic AI，则很可能成为这一体系中的“数字神经中枢”。

结语

微软与诺基亚此次发布的白皮书，其实揭示了一个越来越清晰的现实：随着 AI 深入网络核心，未来运营商不仅需要更强大的网络能力，更需要一套能够自主感知风险、自主分析威胁并快速响应的 AI 安全体系。

这意味着，通信行业正在从“自动化网络”迈向“自智化网络”，而安全体系也必须同步完成智能化升级。

对于全球运营商而言，这场变革已经不再是“是否开始”的问题，而是：谁能更快进入 AI 驱动的自智网络时代。