证券代码：300921　　证券简称：南凌科技

南凌科技股份有限公司
投资者关系活动记录表

编号：2025-004

投资者关系活动类别	√特定对象调研□分析师会议 □ 媒体采访□业绩说明会 □ 新闻发布会□ 路演活动 □ 现场参加□其他
参与单位名称	国信证券、申万菱信基金
时间	2025 年 5 月 21 日 11:00-12:00
地点	公司总部会议室
上市公司接待人员	董事会秘书喻荔女士
投资者关系活动主要内容	公司董事会秘书喻荔女士简要对公司 2024 年及 2025 年一季度经营状况及主要业务发展情况进行了交流： **1、公司怎么切入国央企市场？** **答：**公司通过生态合作部来切入国央企市场，目前，公司正稳步推动生态合作伙伴体系，截至 2025 年 Q1 公司签约渠道伙伴已达到 70+，主要包括国内外的基础电信运营商、云服务商、集成商和安全厂商，合作模式正逐步由“项目合作“、”资源合作”迈向“产品级合作”，公司通过与生态伙伴的产品级深度合作，为国央企客户以及行业大型企业提供多元化、高品质的“云智网安”一体化解决方案。 公司重点推进与基础电信运营商的深度合作。目前已启动与中国联通、中国电信的产品共创和网络能力共建工作，南凌科技骨干网目前正分阶段与基础电信运营商的骨干网进行互联互通对接，公司将基于运营商网络的低时延和高冗余优势，构建南凌科技央国企专网，此方案有利于充分发挥运营商骨干网络的健壮性优势和南凌科技骨干网络的灵活性优势。

	与此同时，公司计划适时启动智能服务平台的立项和建设工作，本项目将采用与生态合作伙伴联合研发的模式，以“监控即服务”（MaaS）模式，未来将全面满足央国企客户“多网统一管理、应用级监控和端到端监控”的刚性需求，保障客户对于网络和安全环境的全局可视与实时掌控。 **2、请问公司主营业务成本构成如何？公司有没有什么降本的措施？** **答：**2024 年，公司主营业务成本主要包括：本地网络成本，占主营业务成本的 37.17%；骨干网络成本，占主营业务成本的 22.54%；运维费用、设备折旧及其他，占主营业务成本的 17.87%；设备及软件采购，占主营业务成本的 16.81%；服务采购及其他，占主营业务成本的 5.61%。 为进一步提升公司的运营效率与竞争力，公司已全面启动成本优化工作。由于公司网络架构复杂，涉及多家运营商数千条基础线路资源。并且，网络成本优化是一项系统性工程，需要综合考量线路续约、流量重新分配、设备升级等多个环节，受上述因素制约，优化效果在 2024 年暂未得到明显体现。2025 年第一季度，公司降本增效专项工作效果已经开始显现。2025 年一季度毛利率 33.11%，较去年同期提高 6.33 个百分点，较 2024 年提高 3.31 个百分点，整体盈利能力进一步夯实。后续公司将深化精细化运营，巩固成本管控成果。目前，公司正稳步推进网络成本优化的各项工作，期待通过长期努力降低运营成本，为后续公司业绩增长注入动力，实现降本增效的良好局面。 **3、公司的主要客户类型是哪些？** **答：**2024 年，公司前五大下游客户所处行业分别为：制造业、信息传输、软件和信息技术服务业、批发和零售业、金融业、租赁与商业服务业。其中，制造业占比较大，为 23.45%。南凌科技针对制造行业的数字化转型需求，通过提供 SD-WAN 全球组网服务、云网安一体化 SASE 服务、多云互联与智能运维服务，

	实现技术与场景的深度融合，解决了其智能制造、全球化布局中的网络与安全难题。典型案例是为某光伏龙头企业打造“全球一张网”，实现其全球 50 多个地区的分支机构低延迟互联。该方案突破传统专线限制，支持混合云、4G/5G 等多链路接入，解决制造企业因业务快速扩张导致的网络部署滞后与跨区域传输效率低下问题，使东欧、中东等偏远地区站点实现市内就近接入，数据传输速度获得极大提升，为其全球化业务快速扩张提供了可靠、安全的网络基座。 **4、目前 AI 应用是趋势，公司业务有什么与 AI 结合的地方？** **答：**全球已经进入 AI 驱动的产业革命，随着 AI 大模型的逐渐普及，AI 将对生产生活的方方面面产生深远的影响。AI 不仅能对自身产品和服务能力进行赋能，也能够催生更多安全应用场景和需求。 公司始终关注 AI 大模型发展趋势，并于 2024 年接入智谱、通义千问等大模型，用于内部数据处理、客服问答等场景。DeepSeek 出现后，公司迅速接入 DeepSeek 大模型，基于公司多年累积的网络和安全运营数据，对 DeepSeek 大模型进行本地化部署，完成安全防护大模型 NovaGuard，赋能 SASE 服务，提升公司云智网安一体化服务能力；同时，用 DeepSeek 赋能网络和安全运维的各个环节，提升运维效率和准确性，快速生成客户解决方案，提升运维自动化水平。目前，南凌科技已实现多种 AI 大模型协同应用，为公司产品升级和业务发展注入动力。 不仅如此，公司也积极探索企业客户在 AI 应用场景中对于网络和安全的新需求，例如大型、超大型企业开展 AI 大模型本地化部署时，需要更安全与更高品质的网络将大模型下发到分支机构；大模型推理时，需要就近的边缘计算能力，降低延时，优化用户体验，并需要身份验证和终端安全检测能力，以确保远程连接的安全性等。根据客户在 AI 应用中的新需求，适时推出创新解决方案，赋能企业 AI 应用落地。

	目前 AI 相关产业都处于起步阶段，公司也仅开始针对性研究，暂未产生任何直接收入，敬请广大投资者注意投资风险。 **5、公司对未来网络安全领域的发展怎么看？** **答：**随着 AI 大模型、云计算、物联网等新技术的快速发展，正在全球范围内推动千行百业的革新与重构。网络安全领域也面临新的变化，既有机遇，也有挑战。主要体现在几个方面： 1、AI 技术催生新场景和新业态，推动网络安全市场增量 AI 技术的应用场景正从单一领域向全产业链延伸。工信部预测，AI 驱动的场景化安全需求将成为中国网络安全市场的核心增长点。业务场景的智能化升级对系统的安全防护、数据隐私保护提出了更高要求。同时，攻击者利用生成式 AI 伪造钓鱼邮件、自动化渗透工具，使得勒索攻击、供应链攻击更加隐蔽，安全防御难度升级。这也将推动 AI 赋能的 SASE 解决方案更快速普及，实现主动防御、智能决策和高效运维，为 AI 时代提供更符合需求的网络安全服务。 2、网络安全技术持续革新，加速向云化、服务化转型 近年来，越来越多企业的 IT 架构向云端迁移，传统的防护模式难以适应动态化、无边界化的网络环境。云原生技术的发展要求安全能力与云平台深度集成，云安全服务成为趋势。云安全服务强调云化管理和服务型的交付模式，与传统本地安全防护相比，具有弹性扩展、高可用、集中管理、快速部署、按需付费等优势，帮助企业真正实现从“被动防御”向“主动运营”的范式转变。 以安全托管服务（MSS）和托管检测与响应（MDR）为代表的订阅式安全服务交付模式已成为主流。MSS 重在安全基座，MDR 更强调主动防御，两者协同互补，日渐趋向融合。两者均为订阅制模式，可依托专业安全运营中心（SOC）实现 7×24 小时全生命周期防护，覆盖威胁监测、漏洞闭环管理及安全编排与自动化响应（SOAR）等核心能力，通过资源池化与能力复用，

	显著降低企业安全运营成本与人力投入，使其聚焦核心业务创新。同时推动安全产业从"产品交付"向"能力服务化"转型，形成专业化分工协同生态，整体提升行业服务标准化水平与运营效率。 3、远程办公常态化与边缘计算爆发，安全边界防护需求快速增涨 Gartner 报告称，全球混合办公员工占比从 2019 年的 20%升至 2024 年的 65%，推动企业对“任意地点安全接入”的需求。IDC 数据显示，边缘设备数量 2025 年达 270 亿台，传统网络无法满足低时延要求，SASE 的全球节点覆盖成为主流。同时，SASE 具备依托零信任身份认证的网络安全接入能力，以及边缘计算能力，可覆盖企业分支、移动终端等多场景需求。 4、云网协同需求持续提升 Gartner 报告显示，78%的企业已实际部署或规划混合云架构，推动"云网安"融合服务需求增长。公司依托 SD-WAN 组网技术及安全能力优势，与头部云厂商深化合作，构建多云/混合云、云网协同、云网安融合服务能力，满足企业多场景业务需求。 **6、公司与各大厂商的云是如何合作的呢？** **答：**全面已经打通国内外云平台，持续扩展与火山引擎、腾讯云、华为云、金山云、京东云、Azure、AWS 等全球主流云平台的深度合作，能够支持全球混合云、多云互联，通过跨平台资源池化，实现全局算力、存储、网络资源灵活动态分配，解决企业数字化转型中的资源碎片化、跨云数据互通、管理困难等问题。
附件清单（如有）	无
风险提示	上述内容如涉及对行业的预测、公司发展战略规划等相关信息，不视作公司或公司管理层对行业、公司发展的承诺与保证，敬请广大投资者理性决策、注意投资风险。
日期	2025 年 5 月 21 日