证券代码：300352　　证券简称：北信源　　公告编号：2026-014

北京北信源软件股份有限公司 2025 年年度报告摘要

一、重要提示

本年度报告摘要来自年度报告全文，为全面了解本公司的经营成果、财务状况及未来发展规划，投资者应当到证监会指定媒体仔细阅读年度报告全文。
所有董事均已出席了审议本报告的董事会会议。
中兴华会计师事务所（特殊普通合伙）对本年度公司财务报告的审计意见为：保留意见。
非标准审计意见提示
☑适用 □不适用

中兴华会计师事务所（特殊普通合伙）为公司 2025 年度财务报表出具了保留意见的审计报告，为公司 2025 年度内部控制有效性出具了否定意见的内部控制审计报告，本公司董事会对相关事项已有详细说明，请投资者注意阅读。
公司上市时未盈利且目前未实现盈利
□适用 ☑不适用
董事会审议的报告期利润分配预案或公积金转增股本预案
□适用 ☑不适用
公司计划不派发现金红利，不送红股，不以公积金转增股本。
截至报告期末，母公司存在未弥补亏损

截至报告期末，公司母公司存在未弥补亏损。
董事会决议通过的本报告期优先股利润分配预案
□适用 □不适用

二、公司基本情况

1、公司简介

股票简称	北信源	股票代码	300352
股票上市交易所	深圳证券交易所		
联系人和联系方式	董事会秘书	证券事务代表	
姓名	王晓娜	张玥莹	
办公地址	北京市海淀区中关村南大街 34 号中关村科技发展大厦 C 座 1602 室；北京市海淀区闵庄路 3 号玉泉慧谷 2 期 3 号楼 4 层	北京市海淀区中关村南大街 34 号中关村科技发展大厦 C 座 1602 室；北京市海淀区闵庄路 3 号玉泉慧谷 2 期 3 号楼 4 层	
传真	010-62147259	010-62147259	
电话	010-62140485-8073	010-62140485-8073	
电子信箱	vrvzq@vrvmail.com.cn	vrvzq@vrvmail.com.cn	

2、报告期主要业务或产品简介

（一）公司主营业务

公司是国内终端安全管理领域的龙头企业，是国内网络与信息安全领域领先的解决方案提供商，为客户提供涵盖网络与信息安全的软件开发、运维管理及系统集成在内的行业级、城市级体系化信息服务解决方案，用户覆盖政府、军队、军工、金融、能源等重要行业单位。目前公司产品体系已形成“信息安全及信创、高安全通信及移动办公、国防智能及生态建设”三大格局，推动公司从传统的终端安全领导者逐步转型为数字经济时代智慧安全的全面产品提供商和解决方案提供商。结合自主研发的高安全通信聚合平台“信源密信”，打造了“北信源 AI 平台”，作为多智能体安全开发平台能够为客户提供大模型 AI 和功能丰富的智能体，既支持私有化大模型又支持外接互联网大模型，如 DeepSeek、千问、火山、Kimi、智谱清言、MiniMax 等国内优秀大模型，该平台可服务于需要人工智能的第三方应用系统。同时，信创产品作为公司重要发展战略之一，公司推出了完整的信创产品体系和解决方案，融合众多信创平台构建了完整的生态链，合力打造信息技术应用创新体系，为行业客户和城市客户提供安全可信的软硬件一体化解决方案，提供更加全面、灵活的信息安全保障，从技术、产品和解决方案等层面积极支持国家信息技术应用创新发展战略，为国家信息安全建设与信创平台发展战略贡献更多力量，为我国数字经济发展保驾护航。

报告期内，公司主营业务未发生重大变化。

（二）主要产品及用途

1、信息安全及信创

随着信息通信技术迭代与数字经济深度渗透，办公场景已演进为 PC 终端、移动终端、虚拟终端、工控终端及行业专用终端等多元算力载体并存的格局，网络接入多样性、数据存储海量化，持续拓展网络安全管理的边界与内涵。在终端安全管理体系由传统的 PC 机管理扩展到智能终端以及各种 IP 设备的泛终端统一管理，北信源作为业界最早建立“泛”终端安全管理体系的安全厂商，实现了对各类型终端的一体化管控；在建立“泛”终端安全管理体系的同时，全面布局了网络接入控制、防火墙、入侵防御监测、网络安全审计等边界及网络安全产品，并随着信创市场的快速发展，北信源全线产品均已发布了信创平台下稳定运行的版本，并为客户提供信创平台下泛终端主机安全、数据安全、边界及网络安全整体解决方案及全系列安全产品，在行业内保持持续快速增长态势。

报告期内，公司加强了在信创及信息安全一体化产品融合，全力打造了新内网安全一体化管控平台，解决了用户内网中各安全系统之间普遍存在着功能重复、兼容性较差的问题，同时同一终端上安装多个安全防护系统，对终端本身资源的占用率偏高，严重影响终端运行及终端用户使用体验。北信源新内网安全一体化管控平台将各种终端类型在多样的系统环境中所面临的复杂安全威胁，通过“一套服务器平台，一个客户端容器”，涵盖系统安全、行为安全、边界安全、网络安全和数据安全等安全领域，各系统采用模块化插入终端容器中，从而达到一体化管理效果。

一体化服务器平台采用 SOA（Service-Oriented Architecture，面向服务的架构)的分布式微服务架构，具备高可用、高性能、高并发、易扩展的特性，模块间松耦合、服务间单向依赖，标准化接口和流程。一体化客户端技术架构实现了终端功能插件化模式，方便管理和加载不同产品功能模块，为终端安全一体化容器提供技术基础，同时对整个终端框架下的功能模块提供数据总线服务，每个模块都可以订阅自己关心的数据，或发送数据到数据总线上，此技术的使用降低了模块间的耦合性，能很大地提高整个客户端的稳定性。新内网安全一体化管控体系采用的是新一代微服务技术体系开发，拥有多项专利技术体系。实现了一个灵活扩展，高度可运维的微服务应用平台，提供大容量、高密级的数据处理和实时监控能力；支持采用分布式级联部署模式，能够适应跨地区的大中型企业里的复杂网络环境，具有良好的伸缩性。

1.1 基于信创平台的全系列安全产品及解决方案

在信创领域，公司始终高度重视自主创新，发挥技术优势，积极响应国家战略部署，遵循国家相关技术规范要求，不断创新并积极与自主创新硬件和软件环境进行适配，目前北信源全线产品均已发布了信创平台下稳定运行的版本，已有多款重要产品通过了国家相关主管部门的检测，分别是北信源主机监控与审计系统、北信源服务器审计系统、北信源

终端安全登录系统、北信源防病毒系统、北信源打印刻录监控与审计系统、北信源运维监管平台、北信源电子文档发文信息隐写溯源系统、北信源电子文档安全管理系统、北信源防火墙系统、北信源数据库审计系统等。

自主创新软硬件平台的普及为公司信息安全产品体系的进一步发展带来了新的契机。公司兼顾分保市场和等保市场布局通讯安全、边界安全、终端安全、数据安全、网络安全、大数据安全，构建了以信源密信为安全通讯底座的一体化安全解决方案，并打造了完善的软件和硬件信创生态圈，实现了 wintel 体系安全向信创体系安全的平滑过渡。公司将与众多信创平台生态链企业一起合力打造创新可靠生态体系，为行业客户提供安全、可信、适用的软硬件一体化解决方案和更加完善、可靠的信息安全保障，为国家信息安全建设与信创平台发展战略贡献更多力量。

1.2 边界及网络安全体系

边界及网络安全体系是北信源信创平台整体解决方案的基础，为内网环境构建了基本的防御环境。边界及网络安全产品体系致力于保障网络边界完整性及网络环境的安全性，主要对接入网络设备、进出网络边界的数据流进行有效的检测和控制，有效的检测机制包括基于网络的入侵检测、边界的内容访问过滤等，有效的控制措施包括网络访问控制、入侵防护、扫描检测、审计溯源等，主要产品包括网络接入控制系统、网络边界监测系统、视频安全监控系统、动态访问控制系统、Web 应用防火墙、高级威胁检测系统、安全运维审计系统、安全日志审计系统、风险监测扫描系统、网络安全审计系统、第二代防火墙、入侵防御监测系统、上网行为管理系统等产品。

报告期内，公司重磅升级网络接入控制系统与网络边界监测系统两大边界安全核心产品，全面强化认证准入、终端安检、资产管控、违规治理等核心能力，深度适配信创环境与多厂商软硬件生态，精准满足政企客户等保、分保及行业合规要求，成功为能源、政务、企事业单位等多领域客户筑牢网络边界安全防线。其中网络接入控制系统凭借多维度安检优化、DHCP 全流程管理、IAM 平台联动等核心能力升级，在身份认证、全终端安检、IP 资源管理、权限管控等领域实现功能突破；通过动态码账号管理、策略路由全代理、IPv6 流量指纹识别等创新能力，构建起从账号准入到网络访问的全链路安全防护体系，同时实现账号生命周期自动化管理、管理员多因素认证加固，大幅提升接入控制的灵活性、安全性与运维效率。网络边界监测系统则以子网 IP 精细化管理、多维度违规管控、全类型探针协同、全场景资产治理为核心升级方向，通过子网自动化分配、IP 高效复用、权限精细化管控等能力优化，实现网络资源的智能化管理；依托违规外联一体化处置、IPv6 串线多网卡检测、Trunk 口摆渡阻断等技术手段，打造从发现到阻断的全流程违规治理体系，同时完善软硬探针协同管理机制、扩展信创探针支持，强化探针探测与网关管控能力；并通过网络拓扑可视化、跨品牌交换机 ACL 适配、全类型资产发现整合，构建起覆盖 IPv4/IPv6 网络、终端、服务器、IoT 设备的全维度资产画像，实现资产属性动态更新与全生命周期管理，为网络边界安全防护提供全方位、精细化的技术支撑。

1.3“泛”终端主机安全体系

公司依托中国终端安全管理市场龙头地位，积极创新、锐意进取，率先建立“泛”终端安全管理体系，将各类终端纳入一体化管控范畴，并将终端安全管理由事件驱动型发展为主动防御型，涵盖终端发现、终端接入管控、安全配置核查、主机加固、安全管理、检测与响应、离网审计、终端运维等全功能的闭环管理体系。主要产品包括安全套件、内网安全管理系统、防病毒系统、主机监控与审计系统、服务器审计系统、终端安全登录系统、操作系统安全加固系统、终端管控系统、终端安全护理系统、主机安全检测响应系统 EDR(Endpoint Detection and Response，端点检测和响应)、特权账号运维管理系统等产品；其中主机监控与审计系统、终端安全登录系统和防病毒系统在市场持续处于领先优势，并在信创领域也取得不菲的成绩。“泛”终端主机安全是北信源信创平台整体解决方案的防护主体，主要目的是为终端主机系统自身构建防御机制。

报告期内，公司聚焦政府、能源、金融、交通、军工等重点行业，升级迭代了基于信创平台全系列终端的安全套件产品，凭借卓越的跨平台适配性与一体化防护能力，赢得各行业用户广泛认可与高度评价，为产品向更多领域市场拓展筑牢根基。本次升级后的终端安全套件，以泛终端主机安全一体化防护为核心定位，深度打造跨平台、融合式管理体系，成功实现对异构终端的统一安全防御与集约化运维管理。产品以防护能力集成化、数据采集管理统一化、安全接口规范化为设计核心，通过基础平台模块化整合身份鉴别、终端接入控制、主机审计、防病毒、外设端口管控、打印刻录监控、介质管控、违规外联监控等全维度防护子系统，采用标准化接口实现与信任服务体系的无缝对接及资源同步，为运维管理、态势感知、监测预警、风险管控等工作提供全量数据来源与高效传输通道。同时，该安全防护体系可与 IT 运维平台、

安管平台、综合审计平台、保密监管平台等多平台联动对接，实现基础数据同步、终端统一认证、主机资产核查及风险联动管控，依托安全产品间的智能联动机制，全面提升网络信息系统的体系化、智能化、动态化安全防御水平与快速响应处置能力；且具备极强的环境适配灵活性，可充分满足物理主机、虚拟化、云服务器等不同部署场景的使用需求，构建起主动防御、动态智能的全场景网络安全防护体系。

1.4 数据安全产品体系

数据是企业信息化的核心资产，所以数据是信创平台整体解决方案的真正防护重心。北信源数据安全产品体系致力于保障内网数据资产的安全，主要以保护用户数据资产为核心，以保障用户数据安全使用为主要防护目标，以敏感信息检测、通道安全控制、数据分类分级、窃密行为分析为手段，对企业内数据实行精准分析精准防护，解决用户关键数据定位难、数据泄密管控难、窃密行为追踪难三大难题。主要产品包括计算机终端保密检查系统、数据泄露防护系统、电子文档安全管理系统、打印刻录安全监控与审计系统、文档发文信息隐写溯源系统、屏幕拍摄泄密溯源取证系统、数据库审计及安全防护系统、数据库内容保密检查系统、数据备份与恢复系统、数据脱敏系统、存储介质信息消除系统、移动存储管理系统及安全 U 盘等产品。数据安全产品已在多个行业广泛推广，并得到市场认可。

报告期内，公司将新一代数据安全管理平台深度融合 AI 大模型、DLP、UEBA、文件标记等前沿技术，紧扣实战化防护需求与国家合规要求，已在政府、能源、金融等重点行业成功落地试点应用。该平台以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及商业秘密、工作秘密保护相关法规为核心依据，全面适配信创环境，可充分满足等保、分保等多维度合规要求，为企业打造覆盖数据全生命周期的智能化、体系化安全防护体系，为行业数据安全治理提供兼具合规性与实战性的全新解决方案。

平台构建起识别、防护、检测、响应、溯源全维度数据安全防护能力，从根源上破解企业“数据家底不清、防护策略不精、溯源分析困难”的行业痛点：依托主动探测、机器学习与大模型深度语义分析技术，实现对终端、服务器、网络、应用中结构化及非结构化数据资产的精准识别，通过智能分类分级辅助构建清晰的数据资产地图，完成敏感数据的动态监测与全量盘点；融合隔离沙箱、零信任架构、数据加密、敏感信息鉴别等核心技术，对终端、传输链路、服务端实施全链路闭环管控，覆盖网络传输、外设输出、AI 平台交互等全泄密场景，有效抵御黑客攻击、内部故意与无意泄密、特权滥用、第三方越权操作等多重风险；基于 UEBA 用户实体行为分析技术，实时监测并智能分析异常数据获取、传输、使用等风险行为，结合明暗水印追踪、文件指纹及 MD5 溯源、文件标识全链路追溯等手段，实现威胁的快速定位、精准阻断与全流程溯源，构建“监测、处置、优化”的全流程智能响应闭环；同时搭载 AI 智能分析引擎，实现数据安全事件分析、敏感文件智能画像、文档外发审批 AI 辅助等功能，还可联动信源密信完成告警实时推送与交互咨询，通过动态策略调控实现多产品策略联防联控，大幅提升数据安全管理的智能化与高效化水平。

1.5 安全大数据分析及安全监管

公司以“大数据驱动内网安全，大数据提升管理效率”为理念，加快大数据技术与现有安全产品的深度融合。充分利用大数据技术不断强化终端安全管理的广度和深度，努力打造以“大数据”技术为指导的新一代内网安全产品生态体系。公司安全大数据分析系统是企业级大数据处理、分析和挖掘平台，结合新监管管理要求，通过采集终端行为、网络流量和安全设备等数据，依托人工智能算法和深度学习引擎，对用户行为和业务数据进行分析评估，帮助企业主动应对威胁和风险，时刻掌握全网安全态势和业务状况。产品主要面向政府、网信、公安、行业主管单位及重要行业企事业单位。基于安全大数据分析系统的衍生产品包括安全管理与态势分析系统、日志收集与分析系统、安全日志审计系统和自监管系统等。

公司积极响应《中华人民共和国保守国家秘密法实施条例》要求，全力推广保密检查监管系统，系统以“关口前移、技术赋能、体系治理”为核心设计理念，深度适配机关单位、军工等重点行业及国家关键信息基础设施的保密防护需求，构建立体化、实战化的全维度保密防线，为国家保密治理体系和治理能力现代化筑牢技术支撑。该系统紧扣“统一监测、检查、处置”核心要求，将管理条文转化为实时监测、智能分析、闭环处置、精准溯源的全流程实操能力，从根源上解决传统保密管理中检查覆盖不全、风险发现滞后、处置流程脱节、溯源取证困难等痛点。系统通过网络化部署模式，可对信创及 Windows 终端、数据库、各类应用服务器及互联网接入口、云数据中心出口等重要网络节点实施常态化安全检查与实时监控，实现终端、应用、数据、流量的保密防护覆盖；一方面可动态追踪敏感文件全操作行为、对即时通信、

移动介质、云盘等全外发通道实施精细化管控，实现违规行为即时拦截与多维度风险研判，另一方面能实时侦测 APT 攻击、木马窃密等恶意行为，结合先进的图片精准识别、多维度溯源取证算法，精准识别各类敏感信息与泄密风险，并快速定位泄密源头、还原事件轨迹，通过规范的流程化隔离、擦除等联动响应，彻底消除泄密隐患。

报告期内，保密检查监管系统搭载智能分析中台与文档分析中台，可实现对结构化、非结构化、半结构化数据的深度扫描与智能分析，同时支持静默检查、一键自查、智能化检查等多元检查方式，为 OA、邮件、打印刻录等办公系统提供综合文档分析服务，进一步强化全场景保密防护能力。目前，该系统已在政府、军工等领域成功落地应用，不仅是公司对国家保密相关法规要求的快速响应落地，更是以技术创新推动保密工作数字化、智能化升级的重要体现，将为我国信息安全和保密防护工作提供强有力的技术保障与实战支撑。

1.6 区块链及相关安全

公司相关战略研发团队已开展了区块链领域的研发工作，其中包括数字钱包的研究和开发工作。公司在积极挖掘与相关金融机构的合作机会，并拓展数字钱包与信源密信的关联技术研发。区块链机能帮助企业简单便捷上区块链，企业只要把区块链机部署在机房服务器（或云服务器）上，就能把电子数据变成区块链数据，区块链机还会记录电子数据产生的时间、产生电子数据的服务器所在地理位置，来保证上链前后数据真实。

区块链机已经在部分行业得到应用和部署，包括航天、环保、司法、行政执法、金融、医疗、教育等行业。生态环境保护需要准确权威的监测数据，环境类电子数据量大且面广，区块链技术可以保障电子数据原装，不可篡改，而且区块链机上链简单，使用方便，能满足环保系统对电子数据固化存证和溯源监管的需求。目前区块链机已经在山东省滨州市生态环境局邹平分局进行试点应用，对该局的环保监测数据进行实时上链存证，为其环保监测执法提供强有力的电子证据支持。除山东邹平外，区块链机还在重庆和衡水部署应用，保障生态环境监测数据的真实完整可信。紧跟数字医疗+区块链优势政策，中国卫生信息与健康医疗大数据学会——信息及应用安全防护分会联合行业企业建立的卫健链，就是以区块链机为节点组链，可覆盖存证溯源、监管、数据协同共享等业务应用场景，支撑健康医疗行业区块链应用需求。教育行业也在不断深化区块链，依托区块链机的优势，公司与杭州电子科技大学进行产学研合作，为“司法可信支撑关键技术与智能化监管平台研发及应用”提供重要科技支撑。

1.7 密码产品体系

公司积极响应国家“密码强国”战略，以构建自主可控的密码技术基座为核心，全面升级商用密码产品矩阵，形成覆盖“数据存储、传输、应用、管理”全生命周期的安全解决方案。通过北信源服务器密码机、云服务器密码机、VPN 安全网关及密码管理平台四大产品的协同联动，公司实现密码技术与新一代信息基础设施的深度耦合。该产品体系以国产密码算法为内核，打通“硬件层密码算力支撑－网络层加密传输控制－平台层密钥智能管理”全链条能力，强化企业在数据加密、身份鉴权、访问控制等核心安全场景的自主可控性。一方面，通过构建云网端一体化的密码资源池，实现跨环境密码服务的弹性部署与统一调度，有效降低客户在多云混合架构下的密码应用复杂度；另一方面，依托动态密钥管理、自动化策略编排等能力，将密码防护深度嵌入业务系统，形成“密码即服务”的新型安全范式。目前方案已通过国家商用密码产品认证，可无缝适配信创生态，满足等保 2.0、关基保护密评等高阶合规要求，可应用于政务大数据、金融核心系统、工业互联网等关键领域。

报告期内，公司核心是围绕 “合规适配、技术融合、场景落地”构建实战化密码安全能力，既响应了国家法规对密码应用的强制要求，也通过与现有安全产品的深度集成，为客户提供一体化、全维度的密码安全防护解决方案，助力各行业客户筑牢数据安全密码防线。

1.8 安全服务体系

公司作为中国信息安全领域的领军企业，深耕行业三十年，始终以“守护数字时代的安全信任”为使命，致力于为政企客户提供全方位、智能化的网络安全解决方案与专业化服务。依托自主研发的核心技术、国家级安全资质及丰富的实战经验，公司构建了覆盖安全咨询、风险评估、威胁监测、应急响应、攻防演练、安全运维等全生命周期的服务体系，助力客户应对数字化转型中的复杂安全挑战。

报告期内，公司参与了多个网络安全服务项目，涉及政府行业、能源行业、金融行业等，主要服务内容为安全评估服务、安全运维服务、等保咨询服务、人员配置管理、安全管理制度、安全教育培训、安全攻防演练、安全应急演练、重保支撑服务、网络安全检查、供应链评估服务、风险评估服务等。通过系统性的安全服务来进一步完善和提升用户系统信息安全保障能力。

2、高安全通信及移动办公

信源密信是公司全力打造的以私有服务器为载体、以安全通信为基础的高安全即时通信平台。该平台全面适配信创环境，支持跨终端、全方位、安全可信的即时通信，是以“即时通信框架，安全通信底座”为基础，为用户提供即时通信、协同办公、应急指挥、任务管理、智能化流程、应用开发、万物互联、互联互通等多层次的安全聚合平台服务，可大幅促进党政军及央国企单位的数字化、移动化、智能化发展进程。

信源密信目前在党政军、国防及智慧建筑领域的应用落地，已经充分验证其作为“信息传输中枢”的可靠性。其“AI+IoT”的社交化框架，可通过自然语言将异构的物理设备转化为可通讯、可指挥的数字化资产，在人工智能和具身智能蓬勃发展的背景下，信源密信作为万物互联的安全通信底座将焕发蓬勃的新动能。

2.1 信源密信具备高安全性

信源密信采用高安全架构设计，遵循“三端加密、五维防护”的安全理念，并使用高可靠性和支持高负载的微服务架构。在客户端，信源密信采用安全加固和动态加解密的安全设计机制，在传输过程中，采用安全传输协议和专用加密算法对数据进行双重加密传输，防止泄密；在服务端，对文件和聊天信息均进行加密保护，支持一人一密、一文一密。加密算法采用国家密码局认可的国密算法。信源密信系统从通信、访问、存储、管理、使用五个维度进行全方位安全防护。

信源密信拥有丰富的安全功能设计，在三端加密、五维防护的安全基础上，还提供账号锁定、三权分立、设备绑定、离线安全、密聊消息、内容保护、阅后即焚、防隐私泄露、文件管控、数字水印、多方安全会议、基于角色的访问控制等特色安全功能。

信源密信支持全面信创适配，是首批实现信创兼容的安全即时通信产品。其服务端和客户端支持银河麒麟、中标麒麟、UOS、鸿蒙等主流国产操作系统；支持龙芯、飞腾、兆芯、海光、申威等国产 CPU；支持东方通、金蝶等国产中间件；支持达梦、金仓、神通、高斯等主流国产数据库；支持国密加密算法。

2.2 信源密信具备高效灵活、实用的功能

产品具备完整的即时通信功能，包括点对点聊天、群聊、语音聊天、语音通话、文件传输、微视频等通用功能。同时支持 PC、手机、Pad 三端同时在线，支持 2000 人以上超大群组，并提供丰富的群管理权限控制及群组自动维护功能。可实现一键建群、批量建群、快速建群、面对面建群、审批建群等多种便捷方式，有效提升群组沟通效率。

此外，还支持群内私聊、阅后回执、密聊、单次阅读、延时消息、未读提醒、V 标好友、会话房间、强制提醒、快捷任务、自定义表情、组合指令消息等多种特色安全功能，进一步提高工作协作效率。

在应用层面，信源密信提供公众号推送、知识问答、培训考核、在线视频等功能，并内置知识库系统，可助力党政军企客户开展内部宣传与学习，沉淀知识经验，打造数智化宣传教育体系。

信源密信支持高度个性化的按需配置，包括单位组织架构显示的安全保密策略、用户标签管理、管理员后台建群，以及自定义界面、自定义主菜单名称等单位个性化设置。

信源密信产品形态多样，支持灵活部署，既可提供私有云或本地服务器的软件版本，也可提供标准机架式软硬一体服务器，还可提供无需固定 IP 的超小迷你服务器。针对集团用户推出多租户版本，满足大型集团企业的分级分域管理需求。

2.3 信源密信具备全面标准的开放开发接口，支持开放扩展

信源密信是一个开放的即时通信底座，既支持小程序、H5、原生应用的快速集成，也支持通过底座快速开发全新业务系统。在密信中发布的应用或以密信为底座开发的系统，将天然继承即时通信能力；同时，业务系统也可调用即时通信接口。通过服务器端 API 可实现新业务系统与密信的互联互通，通过客户端 SDK 可让第三方 App 快速集成即时通信功能。

此外，信源密信还提供开放接口，支持与邮件系统、任务审批、日程管理等标准办公应用无缝集成，用户可以根据自己的需求，添加邮件系统、任务审批、日程管理等多款高质量的标准办公应用，快速实现移动化办公。相比传统独立建设、相互割裂的系统，信源密信一体化平台提供统一的办公门户、统一的组织架构、统一的身份认证、统一的消息待办通知以及统一的业务应用管理，显著提升办公效率和数字化体验。

2.4 信源密信具备 AI 扩展能力，打造智能化工作生态

北信源 AI 平台是信源密信的智能化配套产品，集成了多种开放互联网及私有化部署的大语言模型能力。该平台可有效管理用户对大模型的访问与使用权限，并根据客户需求安全对接第三方大模型，为北信源自身的产品和第三方应用提供强大智能支持，为政府机构和企事业单位带来更智能化的办公体验与业务流程，全面提升信息系统智能化水平。北信源 AI 平台已在“AI 知识库”“装备质量 AI 应用”“财达股市通 APP”等场景实现快速落地。目前已接入 DeepSeek、千问、火山、Kimi、智谱清言、MiniMax 等国内优秀大模型，进一步提升智能交互和信息处理能力。2024 年，公司与中译语通达成战略合作，共同助力国家重大项目“跨语言多模态国防科技产业大模型”建设。2025 年，公司通过公开竞争立项，成功获批北京市科学技术委员会、中关村科技园区管理委员会“中央引导地方专项——多语种端到端语音翻译平台研发及示范应用”课题，并获 500 万元科技经费支持。这些都是对北信源深入研究 AI 技术实力的认可。

信源密信主要服务于有高安全通信需求的单位，已覆盖大型、中小型客户、团体组织及特殊行业客户，成功应用于众多国家重点工程和项目。公司针对不同需求开发了标准版、专业版、行业专用版等多个版本，产品形态包括工作秘密版、涉密版、集团版、一体机、小黑盒、私有云版、高安全通信底座。

依托信源密信底座，公司打造了丰富的衍生解决方案：

（1）应急响应平台：基于《国家网络安全应急预案》等政策，在国家重要部委指导下打造，已应用于网络安全应急响应平台、工控安全应急通信系统等。未来将抓住“十五五”全国应急体系建设机遇，加速推进网络安全应急指挥体系建设。

（2）智慧党建安全平台：围绕“四位一体”核心，定制一体化智慧党建解决方案，以信源密信框架为基础，实现党建工作与业务深度融合，同时保障数据安全。

（3）军事园区智慧安管系统：以智能化、规范化、精确化和平台化为目标，实现军事园区的穿透式检查、网格化管理、流程化处置和一体化治理的安全保密管理，搭建统一的智能安管数字底座，建立人、车、物、密精确管控的智慧安全保密防护体系。

（4）市值分析管理系统：专为上市公司实控人、大股东、董事会及证券事务部门打造，支持市值分析、大股东减持/质押计算、线上视频会议、安全即时通信等功能，可自动生成分析报告，提升资本市场市值管理水平。

（5）中央网信办：配合国家网络安全法，搭建覆盖全国数万个关键基础设施的移动端应急保障管理平台，服务中央及各地网信办、党政机关等机构。

（6）公安部：在全国新一代移动警务网基础上建设互联互通即时通信平台，已在湖北、甘肃、河南、江西、湖南等省份成功部署，并实现全国 80%以上省份之间的互联互通。

（7）财政部：覆盖全国财政系统，部署于业务专网，支持不同级别人员查看对应范围的组织机构，全面适配信创环境。

（8）海南省：采用北信源即时通信开发框架，集群化部署社会化治理平台，助力海南自贸区（港）社会治理能力提升，实现“一线放开、二线高效管住”目标。

（9）爱传(AITran)：公司携手生态伙伴爱传智胜的“爱传(AITran)”跨语言交流工具，成为中国文化和旅游部“你好！中国”国家旅游形象推广活动语言翻译服务的唯一供应商。爱传(AITran)致力于为政务、商务、文旅、会议、教育

等多语场景提供高精度、高效率的语言沟通解决方案。爱传不仅满足各种大语种 AI 翻译能力，还支持小语种国家语料库接入，获得小语种 AI 同声传译能力。

公司还组建高水平区块链团队，依托信源密信开展数据存证、健康医疗、社区管理等应用研发。目前，信源密信作为保护国家秘密、工作秘密、商业秘密、个人隐私的安全通信底座，已实现私有化部署、全信创兼容，广泛应用于党政机关、国家部委、国防军工、科研院所、金融机构、能源、医疗等高安全需求领域，被多家单位指定为“指定安全通信平台”。

信源密信荣获首批“办公即时通信软件安全能力”最高级别“卓越级”认证，并首批获得“涉密信息系统”产品检测证书。产品已为党的二十大会场提供安全通信技术保障，是国家重要单位、重点工程及重大会议活动的优选即时通信平台和底座，装机量达千万级别，深受行业用户高度认可。

在“十五五”规划期间，北信源制定通过信源密信切入硬件生态的战略，把核心产品从“应用层”向“基础设施层”进行跃迁，通过 AI 能力和安全即时通信能力融入各行业，深度控制硬件连接与信息流转，在国防与关键基建领域建立起不可逾越的竞争门槛，信源密信将从一个“安全即时通信软件”升级为“全球硬件的数字指挥中枢”。

3、国防智能及生态建设

在信息化与智能化深度融合的新时代背景下，国防安全正面临前所未有的复杂挑战。无人机渗透、网络攻击、低空威胁等非传统安全风险日益凸显，传统防御手段亟须向智能化、体系化、生态化方向升级。北信源国防智能及生态建设，通过基于信源密信为底座的智能安管平台，按照穿透式检查、网格化管理、流程化处理、一体化治理的安全保密管理要求，在园区内外及办公区域构建三重防御手段，搭建统一的园区智能安管“数字底座”，形成集人、车、物、密精确管控于一体的安全保密防护体系。智能安管系统基于国产化软件和硬件环境、采用模块化设计、标准化接口方式研发，汇集预约申请、安检检测、视频监控、载体管控、违规行为告警等数据信息，形成集态势显示、运维管理、授权审核、事件处置、综合评估于一体的安管“智慧大脑”。联邦学习、多方安全计算（MPC）等技术减少数据清洗、脱敏及合规审核的投入，数据协作效率提升。聚焦信源密信在军队方向的创新应用，从智能安防、流程管理、态势感知、低空防御四大维度，系统阐述其在国防安全领域的战略价值与实践路径。

3.1 智能安防体系：构建多层级防御矩阵

国防设施与军事基地的安全防护是军队智能化转型的基础。信源密信通过“三重复合防御+智能权限管理+设备通联平台”模式，打造立体化、全时域的安全屏障。

1）三重复合防御机制

第一重：外围全域感知。依托高灵敏度传感器与频谱探测技术，在军事园区外围部署智能监测网络，实时捕捉火灾、入侵、电磁干扰等异常信号。例如，通过红外热成像与烟雾报警联动，可在火灾初发阶段实现秒级预警，为应急响应争取黄金时间。

第二重：内部精准定位。在园区内部署 RFID 多维检测节点与感温探测器，结合 AI 算法对人员轨迹、设备状态进行动态分析，快速定位异常点位。例如，人员出现在权限不符的位置或者在异常时间出现，平台通过预警、告警转人工处置。

第三重：重要区域权限管控。在办公区、指挥中心等重要区域，采用生物识别与动态密钥技术，实现人员权限的精细化分级管理。通过“一人一密、一事一码”的加密机制，确保敏感信息仅限授权人员访问，杜绝数据泄漏风险。

2）智能设备协同管理：信源密信平台集成消防系统、紧急照明，梯控系统等设备状态数据，通过边缘计算节点实现本地化决策。例如，当烟雾报警器触发时，系统可自动规划最优逃生路径，并控制电梯停运、门禁解锁，确保人员快速疏散。

3）智能设备通联平台能力

作为安防体系的神经中枢，信源密信智能设备通联平台实现多源异构设备的统一接入与协议互通，打破传统安防子系统间的信息孤岛。平台支持国标 GB/T 28181、ONVIF 等主流安防协议，以及 MQTT、CoAP 等物联网协议，可无缝接入视频监控、门禁控制、消防报警、环境监测等十余类智能设备，实现跨厂商、跨系统的互联互通。

平台具备实时数据融合能力：通过统一的数据总线，将分散在各子系统的设备状态、告警信息、视频流等多维数据进行实时汇聚与关联分析，构建全域安防数字孪生体。例如，当入侵报警触发时，平台可自动调取周边摄像头画面、关联该区域门禁出入记录、叠加电子围栏状态，为指挥人员提供全景态势感知。

平台具备智能联动编排能力：支持可视化规则引擎，用户可灵活配置"如果-那么"自动化响应策略。如"周界入侵→就近摄像头转向预置位→启动声光告警→推送移动端→启动电子地图追踪"的多级联动，响应时延控制在毫秒级，实现从"人工处置"到"自动闭环"的跨越。

平台具备安全加密传输能力：基于信源密信自研的加密通信协议，所有设备指令与数据流均经端到端加密传输，防止中间人攻击与数据篡改，确保军事安防网络的通信安全与指令可信。

3.2 流程智能化：重塑系统审批与资源管理体系

内部的人车管控与资源调度效率直接影响战备能力。信源密信通过“表单自动化+流程可视化”技术，推动单位管理向数字化、敏捷化升级。

1）人员通行审批系统

智能表单创建：支持人员车辆信息、通行权限的快速填报与自动核验，减少人工录入错误。

实时进度追踪：指挥中心可通过态势大屏实时查看审批进度，并对超时任务自动催办，提升跨部门协同效率。

2）装备与物资管理：结合 RFID 与物联网标签技术，实现文件、终端设备、灭火器、无人机反制设备等物资的全生命周期管理。例如，所有文件或设备的进出皆在系统审批定级，并可以感知位置以及最终位置的闭环管理。

3.3 态势感知中枢：实时监控与智能决策

信源密信的“神经中枢系统”通过物联网与大数据技术，将分散的安防设备整合为统一作战网络，实现“全域感知、精准决策”。

1）实时监测与预警

消防态势大屏：集成火灾报警设备、感温探测器等数据源，动态展示各区域风险等级，并通过 AI 模型预测火势蔓延趋势。

智能预警推送：当检测到异常信号时，系统自动向指挥中心、巡逻人员及周边单位发送加密指令，形成多层级响应链路。

2）数据驱动的应急响应

精准定位：结合 GIS 地理信息与北斗定位，快速锁定事故点位，并调取周边监控画面辅助决策。

自动化处置：例如，在火灾场景中，系统可远程启动喷淋装置、关闭通风管道，并调度无人机进行空中监测，最大限度降低损失。

3.4 低空防御体系：反制“低慢小”威胁

针对无人机、航空模型等低空慢速目标的渗透风险，信源密信构建“侦-控-打”一体化防御网络，筑牢空域安全防线。

1）频谱探测与信号分析

无人机通信感知：部署云台式频谱探测器，实时捕获无人机上下行信号特征，通过机器学习算法识别敌我目标。

多频段干扰技术：采用高斯集成干扰器，发射定向电磁波阻断无人机导航与控制信号，迫使其悬停或返航。

2）侦打一体实战应用

手持式干扰设备：士兵可通过侦打一体手持终端，快速锁定目标并发射干扰脉冲，适用于战场机动反制。

智能物联平台：所有反制设备接入统一管理平台，实现任务分发、数据回传与效能评估的全流程自动化。

3.5 生态化应用：技术融合与协同创新

信源密信通过开放架构与标准化接口，推动国防智能生态的共建共享。在国防智能化与数字化转型进程中，即时通信不仅是信息传递的工具，更是构建高效、安全、协同的军队生态办公体系的核心枢纽。信源密信即时通信系统通过“端到端加密+智能协同”技术，为军队日常管理、跨域协作、应急指挥提供全场景支撑，推动军事办公从“流程驱动”向“数据驱动”跃升。

1）技术融合创新

5G+边缘计算：以“云-边-端”三级架构，在边境哨所、野外营地等极限环境部署轻量化边缘节点，将 5G 大带宽与本地异构算力融合，使侦察影像、雷达点云等 TB 级数据在前端即完成压缩、解析与决策，端到端时延降至 10 ms 以内，真正做到“数据不出营，感知零等待”。

数字孪生+空间计算：构建基于数字孪生的“虚拟园区”模型，通过空间计算技术实时映射物理营区的装备状态、人员分布与环境参数。指挥员可在 3D 可视化界面中模拟兵力调动、推演战术方案，并同步至即时通信群组，实现“孪生体－实体”秒级联动。

2）军地协同生态

与科研机构、民用企业联合研发，推动反无人机技术、智能消防设备等成果的军民两用转化。例如，安徽省“低慢小”探测反制系统已成功应用于军事演习与城市安保，验证了技术通用性与可靠性。

信源密信即时通信系统通过开放 API 与标准化协议，与民用通信技术、工业互联网平台深度融合，推动“军技民用、民技军用”的双向赋能。

军民协同创新：与头部科技企业共建联合实验室，将 5G 切片、边缘计算等民用技术适配军事场景，提升通信系统的兼容性与扩展性。

战训一体化平台：以即时通信为神经脉络，搭建“云-边-端”协同的虚拟演兵场：士兵佩戴轻量化 XR 头显即可接入跨兵种数字孪生战场，毫米级动作捕捉与 8K 实景渲染让地形、天候、敌情实时同步；指挥员通过同一通信流在 3D 沙盘上圈选、标绘并秒级推送到单兵 HUD，战术调整与前线反馈双向闭环，实现“图上即战场、令下即行动”的战训跃升。

智慧军营：把通信、安防、能源、后勤四大域的数据流统一汇入数字底座，形成一张“军营活地图”：哨兵人脸识别与电子围栏异常秒级告警，光伏微网负荷 AI 预测后自动并网，车辆、弹药、被装 RFID 轨迹实时可视；指挥舱 120 Hz 超宽屏一屏呈现全域态势，鼠标一点即可联动门禁、广播、无人机，真正达成“态势一屏感知、业务一网通办、指令一键直达”的数智军营新范式。

3）安全通信：筑牢军事机密防护屏障

量子级加密传输：信源密信采用量子密钥分发（QKD）与国密算法双重加密技术，实现语音、文本、文件等数据的端到端加密传输。即使通信链路被截获，攻击者也无法破解内容，确保作战指令、部署计划等核心信息零泄漏。

动态权限分级：构建“身份－任务－场景”三维动态权限引擎，实时读取数字军衔、作战角色、密级标签与地理围栏等多维因子，毫秒级生成最小可用权限。战略指挥员拥有“一人一密”量子密钥会话，可直接穿透加密隧道下达绝密指令；普通士兵则自动降级至“只读－定向”通道，仅能接收经语义脱敏后的执行任务包，从协议栈底层阻断一切越权访问，实现“权限随岗而动、信息依令而行”。

4）智能协同：赋能跨域作战与资源调度

多模态通信融合：支持文字、语音、视频、AR/VR 全场景交互，满足前线侦察、远程指挥、虚拟沙盘推演等多样化需求。例如，在联合演习中，指挥中心可通过 AR 眼镜将战场态势实时叠加至士兵视野，实现“所见即所得”的战术协同。

AI 助手辅助决策：在通信流中内嵌大模型语义引擎，对语音、文本、图片进行毫秒级解析，自动抽取时间、坐标、兵力、装备等 28 类核心要素，实时生成可机读的任务 JSON。当指挥员说出“A 区域需 3 辆装甲车”，系统即刻在数字沙盘上标绘最短机动路径，并自动向装甲营、油料组、道路保障分队并行下发调拨工单，全程零人工录入。

跨平台无缝对接：与现有军事管理系统（如人车审批、物资调度、消防中枢）深度集成，打破信息孤岛。例如，应急指挥中，消防报警信息可一键同步至通信群组，并联动地图标记火点位置，加速多部门联合响应。

5）敏捷办公：重构军队行政与任务管理

任务流自动化：通过 RPA（机器人流程自动化）技术，将通信指令自动转化为待办任务。例如，指挥员在群组中发送“明日 10 点检查 B 基地战备状态”，系统自动创建巡检任务、分配责任人并设置提醒，减少人工转译误差。

智能会议中枢：支持语音转写、多语种实时翻译、会议纪要自动生成等功能，会议语音转写准确率≥98%，并实时生成多语种字幕；大模型自动提炼决策要点、风险项与行动清单，30 秒输出双语结构化纪要。多国联合军演场景下，法语、英语、中文等可同屏对照翻译，指挥员一键即可将译文及原文推送到作战终端，实现“说即所得、译即可用”的零时差决策。

全域机动终端：深度适配军用加固平板、战术腕表、单兵 AR 眼镜等全形态设备，内置国密算法与抗量子加密套件，支持离线密话、断点续传与 7 日超长续航。无网环境下，终端自动组建 256 节点自愈合 Mesh，跳频抗干扰速率≥2 Mbps，确保小队在山地、隧道或强电磁屏蔽区仍可加密通播、协同标图，指令零丢失。

AIGC+知识图谱：在即时通信中嵌入 AIGC（生成式 AI）引擎，实时解析群聊、会议语音与文档，自动生成“战术知识图谱”。当指挥员输入“高原寒区补给方案”关键词，系统即刻关联历史战例、地理气候数据与当前库存，生成图文并茂的决策草案并推送至责任人，实现“边聊边生成、边生成边执行”的敏捷闭环。

6）应急指挥：打造“平战一体”响应体系

战时紧急通信通道：预设“红色警报”模式，以 AI 驱动的频谱感知引擎为核心，实时监测干扰强度与网络健康度。一旦判定链路受损，毫秒级跳频至军用抗干扰频段，并同步唤醒低轨卫星/量子中继双冗余链路；高优先级指令自动封装为量子加密小包，抢占星上转发时隙，确保“断网不断链、干扰不扰令”。

智能态势同步：结合神经中枢系统的实时数据，通信平台可动态推送战场态势图、物资库存、人员位置等信息。例如，在反恐行动中，指挥员可通过移动终端查看实时热力图，快速调整兵力部署。

一键联动处置：集成应急预案库，当接收到“无人机入侵”“火灾警报”等特定关键词时，系统自动触发反制设备启动、门禁管控、疏散广播等操作，实现“通信即指挥、指挥即执行”的闭环管理。

星链+量子中继：与低轨卫星互联网（星链/虹云）及量子中继实验网打通，当本地通信节点遭致瘫攻击时，系统自动切换至“星链+量子密钥”双冗余链路：星链提供全球随遇接入，量子中继确保密钥在卫星跳传过程中不可被窃听，实现洲际级指挥链路的秒级恢复与绝对安全。

信源密信即时通信系统以安全为基石、以智能为引擎、以协同为纽带，重新定义了军队生态办公的范式。不仅是信息传递的“高速公路”，更是连接指挥链、作战链、保障链的“超级神经”，为国防智能化注入敏捷性与生命力。未来，随着量子通信、数字孪生等技术的深度融入，军队智能化防御体系将更加自主、协同与韧性。信源密信不仅是技术工具，更是国家安全战略的重要支点，其应用前景必将为国防现代化注入澎湃动能，为打赢信息化战争提供坚实底座，护航大国崛起之路。

（三）经营模式

公司始终高度重视企业文化建设，立足数字化时代核心诉求，恪守“信息之源、信任之源、信心之源、信念之源”的品牌理念，矢志践行“为中国数字化腾飞保驾护航”的企业使命。以“成为全球信息安全领域最值得信赖的领导者”为愿景，我们秉持内修“奋斗、创新、实干”精神，外塑“信任、专业、卓越”的核心价值观，将保障信息安全视为核心责任，坚持螺丝钉精神，以人为本、锐意开拓、精益求精。2025 年，公司进一步巩固终端安全市场龙头地位，全面确立高安全通信及国防智能领域的领军优势，为构建可信赖的数字世界贡献力量。

在产品研发方面：公司自成立以来，一直将自主创新作为发展的根本，在业界首次提出“泛终端安全”理念，并对其开放体系架构、终端及应用防护关键技术、规模化部署管理进行了持久的研发投入，开发了具有自主知识产权的全套终端安全防护产品体系，针对行业客户形成了完整的个性化解决方案集。2025 年，公司坚持以 AI 创新为核心引擎，深化技术与场景融合。特别是公司持续十余年投入研发的信源密信产品，开创安全通信系统工程先河，致力于在通信中保护国家秘密、工作秘密、商业秘密和个人隐私。作为移动安全通信底座，为用户提供了即时通信、协同办公、应急指挥、任务管理、智能化流程、应用开发、万物互联、互联互通等多层次的安全聚合平台服务，满足数字政府建设的通信场景化核心应用，全面支持实战化信创环境，该产品已在国家党政军等重要单位中实现规模化深度应用，多次获得表彰，正加速成为党政军国央企等重要单位移动互联网的基础设施。经过三十年的沉淀，公司已经成长为一家集前沿技术研究、安全产品体系化研发、安全咨询服务于一体的信息安全领军企业。百尺竿头更进一步，公司从市场客户的需求出发，结合自身领域优势，确立了信息安全及信创、高安全通信及移动办公、国防智能及生态建设三大战略成为公司未来的发展方向。

在市场销售及服务方面：公司作为中国终端安全市场的龙头企业，已累计 17 年稳居中国终端安全管理市场占有率第一，具有强大的市场号召力和品牌影响力。公司坚持以客户为中心，以市场为导向，从大区域、大行业、大客户的共性需求出发，同时兼顾中小型用户的个性化需求，制定了基于行业和区域的矩阵式营销管理体系，建立了完整的产品服务体系，配备了一批高素质的专业技术支持人员和客户服务人员，能实时快捷响应客户需求。凭借优秀的产品体系、强大的研发能力、完整的解决方案、良好的售后服务，公司获得了广大客户的信任，建立了良好稳固的合作关系，目前客户群已涵盖 90%以上的政府和行业部门，为我国的数千万终端提供智能、完善的安全服务，特别是高安全的即时通信平台——信源密信产品已经成为国家重点单位、国家重大工程、国家重要活动优选的移动安全通信底座，且在众多重要单位中规模化使用。公司构建以信源密信为核心的数字生态体系，在与生态伙伴深化技术协同创新的同时，合力拓展市场与业务落地。

公司始终采取“集中管控、专业经营、精细管理”的模式，有力地推动公司业务提升和管理优化。随着财务、采购、销售的集中管理和各项规范流程的完善和执行、数字化管理控制平台的完善以及管理工作的推进，2025 年公司进一步深化数字化转型，优化资源配置，进一步完善了管理机制，夯实了管理基础，提升了管理运营效率，使公司的规范化经营水平迈上了一个新的台阶。

（四）主要业绩驱动因素

在全球数字化浪潮加速演进的背景下，网络安全已上升为事关国家安全、国家主权与社会长治久安的关键议题，国家对网络安全的战略重视与顶层部署持续强化，信创大战略顶层设计逐步落地。近年来国家密集出台网络安全、数据安全、数字经济相关法律法规与政策规划，构建起全领域、全流程、全生命周期的政策保障体系，推动各行业网络安全投入持续提升；同时行业安全需求从合规导向向攻防实效导向迭代，新兴技术与新场景催生多元安全需求，叠加公司核心技术、产品与服务能力精准适配市场趋势，形成政策驱动、需求牵引、能力支撑的三重业绩驱动因素，推动公司主营业务持续发展。

1、国家政策体系持续完善，行业发展获顶层战略支撑

网络安全作为数字经济发展的重要保障，已被纳入国家核心发展战略，从 2017 年《中华人民共和国网络安全法》施行起，国家持续出台覆盖基础立法、细分领域规范、产业发展规划、顶层布局设计的系列政策，构建起系统化、多层次的政策体系，为网络安全行业发展奠定坚实制度基础。

2019 年《信息安全技术 网络安全等级保护基本要求》2.0 版本出台，推动网络安全建设向精细化、体系化升级；2020 年十九届五中全会将国家网络空间安全纳入全国百项重点项目，确立网络安全在数字化发展中的核心地位；2021 年《中华人民共和国数据安全法》发布，奠定数据安全产业发展的法律基础，“十四五”规划纲要进一步明确“加快数字化发展，建设数字中国”，提出强化网络安全防护与关键信息基础设施保护要求。

2022 年政策向数字经济、数字政府、政务大数据细分领域延伸，《“十四五”数字经济发展规划》《关于加强数字政府建设的指导意见》等文件，明确强化数字安全体系、构建全方位安全保障体系的核心要求，推动政务、产业领域安全防护需求落地；《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》则明确数据四大基础制度，推动数据要素安全合规流通。

2023 年政策聚焦产业发展与数字中国整体布局，《关于促进数据安全产业发展的指导意见》设定数据安全产业阶段性发展目标，《数字中国建设整体布局规划》将强化数字安全屏障纳入核心能力建设，《“数据要素×”三年行动计划（2024—2026 年）》进一步释放数据安全相关业务市场需求。

2024 年修订后的《中华人民共和国保守国家秘密法》公布，提升国家网络信息系统安全防护标准，压实党政军、国防等领域保密与安全责任；2025 年政策向细分领域、新兴赛道持续深化，《网络数据安全管理条例（修订版）》《关于进一步加强工业领域网络安全工作的指导意见》等文件细化各领域监管要求，《重要军工设施保护条例》首次以法律形式将军工产业链全链条纳入保护体系，为军工信息化等领域带来显著制度保障与市场机遇，“十五五”规划建议则明确加强网络、数据、人工智能等新兴领域安全能力建设，为行业智能化、体系化发展指明方向。

国家政策从基础立法到细分规范、从通用领域到特色赛道、从合规要求到能力提升的层层递进，持续推动各行业加大网络安全投入，为行业发展带来持续、稳定的政策机遇。

2、行业需求迭代升级，新兴场景催生增量市场空间

网络安全行业的发展与新安全威胁、新技术应用、新业务场景同步推进，新威胁的持续涌现推动行业技术与监管体系不断优化，也带来市场需求的持续增长，行业整体需求呈现从合规导向到攻防实效、从通用防护到场景化防护、从基础安全到新兴安全的三大升级趋势。

数字经济时代，市场对网络安全的需求已从传统的满足政策合规要求，逐步转向关注攻防实际效果，愈发重视安全产品和服务能否对大数据、人工智能、移动办公、云计算、工业互联网等新场景实现有效防护，保障系统和数据资产的全维度安全。同时，区块链、生成式 AI 等新兴技术的发展与普及，推动企业业务、设备及网络的融合程度持续提升，也引发信息泄露、深度伪造等新型安全问题，AI 内容安全、数据隐私保护、机密计算等新兴安全需求持续涌现，为行业打开新的增长空间。

此外，政企信息化、数字化建设的持续推进，使得政府、企业等主体对移动办公的信息安全保障需求呈高速增长态势；而网络安全分级保护要求升级、《重要军工设施保护条例》落地等政策落地，进一步推动军工、政务、工业等核心领域对智能化、体系化、全链条安全防护解决方案的需求显著提升，细分领域市场空间持续拓宽。

3、公司核心能力精准适配市场，高效把握发展机遇

面对网络安全行业的政策导向与需求升级趋势，公司凭借深厚的技术积淀、成熟的市场布局及完善的服务体系，形成与市场发展高度契合的核心竞争力，精准把握行业发展机遇，将政策红利与市场需求有效转化为业务发展动力。

公司始终保持对新型安全威胁与行业技术趋势的敏锐洞察，积极应对人工智能等新兴技术带来的全新安全挑战，坚持以市场需求为导向开展技术研发与产品创新，持续加大前沿技术的探索与应用力度，不断提升产品与服务的安全防护能力，以技术创新筑牢业务发展根基。同时，公司依托良好的品牌效应、健全的销售渠道，在党政军、国防、高安全通信、移动办公等核心领域构建起显著的竞争优势，能够快速响应各领域客户的智能化、体系化安全防护需求，为客户提供贴合实际场景的安全解决方案。此外，公司紧跟国家网络安全战略与信创发展部署，持续完善公司治理、强化市场开拓与团队建设，不断提升运营管理效率与市场覆盖能力，全方位承接各领域安全防护需求，推动公司主营业务实现持续、稳定、健康发展。

综上所述，国家网络安全政策的持续深化为行业发展提供了坚实的制度保障，行业需求的迭代升级与新兴场景的拓展打开了广阔的市场空间，而公司在技术创新、综合优势、战略布局等方面的核心能力，精准适配了政策导向与市场需求。三者有机结合构成了公司业绩核心驱动因素，未来公司将继续紧扣数字中国建设与网络安全国家战略，深挖细分领域市场需求，持续强化技术创新与服务能力，以数字化、网络化、智能化赋能高质量发展，推动公司业务实现新的突破。

（五）行业格局及公司所处行业地位

1、行业发展总体趋势

公司所处的软件和信息技术服务业作为“战略性新兴产业”，持续获得国家产业政策支持。数字经济在中国 GDP 比重的稳步提升，随着人工智能、云计算、大数据、物联网、区块链等新兴技术的蓬勃发展，网络安全、数据安全、隐私保护、关键基础设施安全性等安全问题也不容忽视。中国信息通信研究院发布的《中国数字经济发展研究报告（2024 年）》显示，数字经济占 GDP 比重进一步提升至 45.8%，新兴技术与各行业的融合不断加深。其中，人工智能大模型在

政务、金融、医疗等领域的应用场景持续拓展，带动了对 AI 安全、模型安全等新型安全服务的需求。同时，工业控制系统的安全防护成为行业关注焦点。零信任架构在政府和大型企业的落地速度加速。

习近平总书记在 2014 年中央网络安全和信息化领导小组第一次会议上指出“没有网络安全就没有国家安全，没有信息化就没有现代化。”网络安全政策法规的持续完善优化，使得网络安全市场规范性逐步提升。国家已把信息化和网络安全列入了国家发展战略方向之一。2019 年《网络安全技术-网络安全等级保护基本要求》（简称“等保 2.0”）正式公开发布，等保 2.0 覆盖工业控制系统、云计算、大数据、物联网等新技术、新应用，为系统安全工作提供了方向和依据。2020 年中国共产党第十九届中央委员会第五次全体会议审议通过了《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》，该建议强调加快数字化发展，并着重于建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范，同时将国家网络空间安全纳入“一百个重点项目”。2021 年“十四五”规划进一步提出“加快数字化发展，建设数字中国”的目标，并明确指出“加强网络安全保护”和“全面加强网络安全保障体系和能力建设”。2022 年国务院发布的“十四五”数字经济发展规划旨在把握数字化发展的新机遇，推动数字经济健康发展，并强调了建立健全数据安全治理体系、研究完善行业数据安全管理政策、提升重要设施设备的安全可靠水平、增强重点行业数据安全保障能力、支持开展常态化安全风险评估以及加强网络安全等级保护和密码应用安全性评估的重要性。随着数字经济快速发展和政策法规的支持，网络安全产品的需求程度逐渐提升，为行业的持续发展奠定了基础。2024 年全国人民代表大会常务委员会公布了修订后的《中华人民共和国保守国家秘密法》，该法的修订旨在通过科学的管理和技术的创新，提升国家网络信息系统的安全防护能力，加强保守国家秘密，维护国家安全和利益，保障改革开放和社会主义建设事业的顺利进行。2025 年《网络数据安全管理条例（修订版）》正式发布，进一步明确了数据跨境流动的安全管理要求，强化了数据处理者的安全责任；工业和信息化部印发《关于进一步加强工业领域网络安全工作的指导意见》，提出到 2025 年底，工业企业网络安全防护能力显著提升，重点行业工业控制系统安全保障体系基本建成；国家网信办发布《个人信息保护合规审计管理办法》，规范个人信息保护合规审计活动，督促个人信息处理者履行个人信息保护义务。国务院、中央军委发布《重要军工设施保护条例》，聚焦重要军工设施安全防护，明确设施保护范围、各方监管职责与管理单位主体责任，细化保护区管控、安全防护、应急处置等核心要求，筑牢军工领域安全与网络数据安全双重防线，压实相关单位安全保密与防护履职义务。这些政策的出台为网络安全行业带来新的发展机遇，推动行业需求持续增长；

“党的二十大”提出建设网络强国、数字中国等目标，指明了产业建设重点方向。随着人工智能、云计算、大数据、物联网、移动互联等新兴技术不断发展，网络空间成为继海、陆、空、天后的第五空间，推动安全赋能方式从外挂形态向内生形态转变，从烟囱防护式向整合纵深式转变，从边界防御模式向零信任架构转变，从静态防御向动态防御转变，从功能安全、网络安全分离的传统技术路线向一体化解决方案转变，新一代数字安全版图正在成型。

2、公司行业地位

在国家加快建设网络强国、数字中国，持续推进关键信息基础设施自主可控与网络空间安全保障的战略背景下，北信源深耕网络安全领域三十年，始终坚守国家网络安全与数字安全核心阵地，是国内终端安全管理领域龙头企业、网络与信息安全领域领先的解决方案提供商、信创安全领军企业及数字化业务通信安全底座奠基者，行业标杆地位持续夯实。公司累计 17 年位居国内终端安全管理市场占有率第一，长期引领行业技术演进与市场发展，拥有高度行业话语权和市场主导地位；先后承担多项国家级、省部级科研与产业化项目，技术实力与产业贡献获国家层面高度认可，是国家网络安全保障体系的核心支撑单位。

公司紧跟国家信创产业发展战略要求，构建了覆盖全场景的高等级安全资质体系，拥有百余项网络安全专用产品检测、涉密信息系统、军用信息安全、商用密码、信创兼容适配等权威准入认证，是国内资质齐全、安全等级领先的网络安全企业之一。公司持续深化信创布局，已形成超 50 款信创全谱系产品与完整解决方案体系，全面兼容主流国产软硬件生态，构建起自主可控、深度协同的信创安全生态链，在党政、金融、能源、军工等核心信创领域形成显著竞争优势，实现规模化落地，为国家信创产业高质量发展筑牢安全屏障。

依托深厚的技术积淀、完善的资质壁垒及多年行业深耕，公司产品与解决方案广泛覆盖政府、军队军工、能源、金融、国央企等国家关键信息基础设施领域，积累了海量高粘性、高等级核心客户资源，形成难以复制的客户壁垒与品牌口碑。自 2001 年起，公司长期承担全国两会等党和国家重大会议、重大活动的网络与通信安全保障任务，先后荣获国家

科技进步奖、公安部科学技术奖等高等级行业奖项，综合实力与行业影响力稳居行业第一梯队，品牌公信力与行业认可度持续提升。

公司紧扣国家人工智能、卫星通信、国产自主生态体系建设等战略发展方向，坚定推进“信息安全及信创、高安全通信及移动办公、国防智能及生态建设”三大核心布局，深度融合互联网与传统网络安全产业，构建高强度自主安全生态圈。通过聚合上下游优质生态伙伴、产业链投资等方式，完善在 AI 安全、区块链、工控安全等前沿赛道的布局，成功从传统终端安全领导者，全面升级为数字经济时代全场景智慧安全产品与解决方案提供商，全方位适配国家数字经济与实体经济深度融合的发展需求。

公司坚持科技自立自强，以技术创新驱动行业地位持续提升，前瞻布局 AI 安全、纯血鸿蒙、卫星通信、多智能体安全等新一代技术方向，与国内头部人工智能企业深度合作研发“安全+AI”融合产品，聚焦智能威胁检测、数据安全合规等关键领域。核心产品信源密信完成卫星通信适配、鸿蒙生态全维度对接，深度参与国家相关重大标准制定，在党政军及涉密领域占据优势市场地位，成为国家重要单位、重点工程的核心高安全通信平台。目前公司已形成全场景、全谱系、全层级安全产品矩阵，业务向安全通信、云安全、物联网安全等领域全面延伸，可提供一体化行业级、城市级体系化安全服务，持续为我国数字经济高质量发展、国家网络空间安全保驾护航，以全方位安全能力践行网络强国建设的国家战略。

3、主要会计数据和财务指标

（1） 近三年主要会计数据和财务指标

公司是否需追溯调整或重述以前年度会计数据
□是 ☑否

元

	2025 年末	2024 年末	本年末比上年末增减	2023 年末
总资产	1,803,156,253.51	2,168,892,089.69	-16.86%	2,377,881,392.30
归属于上市公司股东的净资产	1,060,299,801.33	1,398,306,590.95	-24.17%	1,543,363,736.91
	2025 年	2024 年	本年比上年增减	2023 年
营业收入	305,856,338.65	516,735,536.88	-40.81%	682,715,630.95
归属于上市公司股东的净利润	-338,007,076.72	-144,784,573.65	-133.46%	6,586,076.58
归属于上市公司股东的扣除非经常性损益的净利润	-344,438,367.75	-145,715,124.10	-136.38%	3,076,433.13
经营活动产生的现金流量净额	28,225,577.27	-72,615,342.52	138.87%	71,990,033.26
基本每股收益（元/股）	-0.2331	-0.0999	-133.33%	0.0045
稀释每股收益（元/股）	-0.2331	-0.0999	-133.33%	0.0045
加权平均净资产收益率	-27.50%	-9.84%	-17.66%	0.43%

（2） 分季度主要会计数据

单位：元

	第一季度	第二季度	第三季度	第四季度

营业收入	61,637,996.68	46,251,776.20	8,124,552.03	189,842,013.74
归属于上市公司股东的净利润	-52,822,515.94	-44,292,069.47	-69,021,650.75	-171,870,840.56
归属于上市公司股东的扣除非经常性损益的净利润	-53,053,472.59	-44,336,372.82	-69,212,558.47	-177,835,963.87
经营活动产生的现金流量净额	3,986,629.60	12,286,904.19	14,955,491.45	-3,003,447.97

上述财务指标或其加总数是否与公司已披露季度报告、半年度报告相关财务指标存在重大差异

□是 ☑否

4、股本及股东情况

（1） 普通股股东和表决权恢复的优先股股东数量及前 10 名股东持股情况表

单位：股

报告期末普通股股东总数	87,913	年度报告披露日前一个月末普通股股东总数	73,682	报告期末表决权恢复的优先股股东总数	0	年度报告披露日前一个月末表决权恢复的优先股股东总数	0	持有特别表决权股份的股东总数（如有）	0
前 10 名股东持股情况（不含通过转融通出借股份）									
股东名称	股东性质	持股比例	持股数量	持有有限售条件的股份数量	质押、标记或冻结情况				
					股份状态	数量			
林皓	境内自然人	15.17%	219,971,355.00	164,978,516.00	质押	77,280,000.00			
南京高科新创投资有限公司	国有法人	1.03%	15,000,000.00	0.00	不适用	0.00			
招商银行股份有限公司－南方中证 1000 交易型开放式指数证券投资基金	其他	0.92%	13,267,900.00	0.00	不适用	0.00			
香港中央结算有限公司	境外法人	0.84%	12,222,646.00	0.00	不适用	0.00			
招商银行股份有限公司－华夏中证 1000 交	其他	0.58%	8,403,000.00	0.00	不适用	0.00			

易型开放式指数证券投资基金						
中国工商银行股份有限公司—广发中证 1000 交易型开放式指数证券投资基金	其他	0.41%	6,011,400.00	0.00	不适用	0.00
胡雯	境内自然人	0.28%	4,045,400.00	0.00	不适用	0.00
瞿文敏	境内自然人	0.27%	3,953,700.00	0.00	不适用	0.00
王坤	境内自然人	0.25%	3,661,100.00	0.00	不适用	0.00
梁明辉	境内自然人	0.24%	3,485,825.00	0.00	不适用	0.00
上述股东关联关系或一致行动的说明	前 10 名股东中，公司第一大股东林皓先生与上述其他股东之间不存在关联关系或一致行动关系，未知其他股东间是否存在关联关系及一致行动人。					

持股 5%以上股东、前 10 名股东及前 10 名无限售流通股股东参与转融通业务出借股份情况

□适用 ☑不适用

前 10 名股东及前 10 名无限售流通股股东因转融通出借/归还原因导致较上期发生变化

□适用 ☑不适用

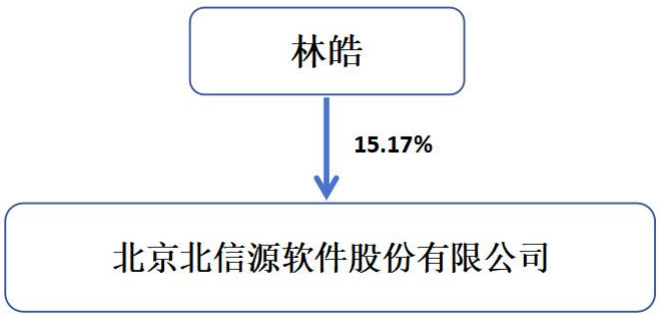
公司是否具有表决权差异安排

□适用 ☑不适用

（2） 公司优先股股东总数及前 10 名优先股股东持股情况表

公司报告期无优先股股东持股情况。

（3） 以方框图形式披露公司与实际控制人之间的产权及控制关系



5、在年度报告批准报出日存续的债券情况

□适用 ☑不适用

三、重要事项

1、2025 年 4 月 18 日，公司召开第五届董事会第六次会议，于 2025 年 5 月 12 日召开 2024 年年度股东大会审议通过了《关于公司 2025 年度向特定对象发行股票方案的议案》等相关议案，根据《中华人民共和国公司法》《中华人民共和国证券法》《上市公司证券发行注册管理办法》《深圳证券交易所上市公司证券发行与承销业务实施细则》等法律、法规和规范性文件的规定，经自查、逐项论证，公司符合向特定对象发行股票的各项条件。具体内容详见巨潮资讯网（http://www.cninfo.com.cn）上披露的公告（公告编号：2025-018、2025-041）。

2、2025 年 12 月 15 日，公司召开 2025 年第四次临时股东会,会议审议通过了关于董事会及换届选举等相关议案，选举出新一届董事会成员，并于当日召开第六届董事会第一次会议，审议通过了选举公司董事长、聘任高级管理人员等相关议案。具体内容详见巨潮资讯网（http://www.cninfo.com.cn）上披露的公告（公告编号：2025-081、2025-082）。