证券代码：300352　　证券简称：北信源　　公告编号：2025-016

北京北信源软件股份有限公司 2024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。

中兴财光华会计师事务所（特殊普通合伙）对本年度公司财务报告的审计意见为：标准的无保留意见。

本报告期会计师事务所变更情况：公司本年度会计师事务所由变更为中兴财光华会计师事务所（特殊普通合伙）。

非标准审计意见提示

□适用 ☑不适用

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。

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、运维管理以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，用户涉及政府、军队、军工、金融、能源等重要行业单位。目前公司产品体系已经完成“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”三大格局的打造，使公司从传统的终端安全领导者逐步成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。同时，信创产品作为重要发展战略之一，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

随着信息通信技术的演进以及互联网的高速发展，日常办公领域出现PC终端、移动终端、虚拟终端、工控终端、各业务专用终端等多类型终端并存发展之势，网络接入多样性、数据存储海量化，进一步使得网络安全管理的范围、内涵和外延在不断扩展，北信源顺应市场潮流，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，是业界最早建立“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后周期市场，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后周期市场，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。

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、智慧入侵防御监测系统、上网行为管理系统等产品。

报告期内，公司发布新版本网络边界监测系统依托主动探测、流量分析、无状态快速扫描等核心技术，在资产测绘领域取得显著成效，系统通过多源数据采集（扫描探测、交换机联动、终端/脚本/硬件探针），累计识别IPv4/IPv6全网资产超2000种类型，覆盖终端、服务器、IoT设备等，动态更新资产属性（IP/MAC/操作系统/服务端口）；基于SNMP协议自动绘制网络拓扑，关联交换机端口与终端接入关系，消除NAT子网、网中网等隐蔽资产盲区，资产识别准确率提升至98%；全面支持信创环境，满足等保及分保要求，助力能源、金融、政府等行业通过资产合规审计。

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、安全配置核查、主机加固、安全管理、检测与响应、离网审计等全功能的闭环管理体系。主要产品包括内网安全管理系统、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，公司依照用户安全保密防护需求构建了基于信创平台的全系列终端安全套件产品，该产品以防护能力集成化、数据采集和管理统一化、安全接口规范化为总体设计目标，将身份鉴别、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、介质管控和违规外联监控等防护子系统通过基础平台进行模块化集成，采用标准化接口与信任服务体系对接，实现资源同步，为运维管理、态势感知、监测预警、风险管控等提供数据来源和传输通道，构建主动防御、动态智能的网络安全防护体系。该产品已应用于政府、能源、金融、交通、军工等诸多行业领域。

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，公司研发了新一代数据安全管理平台，该平台以国家《网络安全法》《数据安全法》《个人信息保护法》等法规为基石，深度融合技术创新与实战需求。通过主动探测与机器学习技术，精准识别结构化、非结构化数据资产，实现分类分级与动态监测，解决“数据在哪、如何防护”的难题。基于隔离沙箱、零信任、数据加密、敏感信息鉴别等技术，对终端、传输、服务端全链路数据进行安全管控，抵御黑客攻击、内部泄露、特权盗用等风险。实时监测异常行为，智能分析泄密风险，结合水印追踪、文件指纹溯源，快速定位并阻断威胁，构建“监测-处置-优化”闭环。该平台全面支持信创环境，满足等保、分保、商业秘密、工作秘密等数据防护要求，为企业打造全生命周期数据安全防护体系，该平台已应用于政府、能源、金融等诸多行业领域。

1.5 安全大数据分析

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。

报告期内，公司研发了基于大数据技术的自监管系统，该系统可以对办公内网或外网的终端、服务器和网络传输中敏感数据进行监测分析，发现窃泄密等异常行为进行处置管理，该系统得到业内广泛认可，已在政府、军工、能源等重要行业应用实施，为国家关键信息基础设施和重要信息系统提供安全保障。

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市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

报告期内，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。

此次密码产品体系的战略布局，标志着公司从网络安全防护向密码基础设施建设的纵深拓展，不仅填补了国产化密码产品在复杂场景下的规模化应用空白，更通过“密码+数据+网络”三维能力融合，为数字中国建设提供具备安全属性的技术底座。未来公司将深化密码技术与人工智能、隐私计算的交叉创新，持续完善密码服务生态，助力国家数字经济安全屏障的构筑。

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，深耕行业二十余载，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，支持全面适配信创环境，跨终端、全方位、安全可信的安全即时通信平台，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，可大幅度促进党政军央国企等单位的数字化、移动化、智能化发展进程。

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，产品遵循三端加密五维防护的安全设计理念，采用安全的微服务架构设计。在客户端，信源密信采用一人一密加密的方式，对文件及数据进行加密处理；在传输过程中，信源密信采用了安全传输协议进行数据的加密传输，防止数据的泄密；在服务端，信源密信对文件、聊天信息都进行了加密存储（一文一密），加密算法采用符合国家密码局认可的国密算法。此外，系统还从通信、访问、存储、管理、使用五个维度进行安全防护设计。

信源密信具有丰富的安全功能设计，除包含常见即时通信软件的安全性功能外，产品还提供了账号锁定、三权分立、设备绑定、一次一密、密码保护、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丰富的特色安全功能。

信源密信支持全面信创适配，信源密信是首批实现信创兼容的安全即时通信产品，信源密信服务端、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，不仅包括点对点聊天、群聊、语音聊天、语音通话、文件传输、微视频等通用功能，还支持PC、手机、Pad三端同时登录；支持2000人以上的群组，支持丰富的群管理权限控制，可实现群组自动维护，支持一键建群、批量建群、快速建群、面对面建群、审批建群等，实现便捷群组沟通；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安全实用的特色通信功能，有效提升工作沟通协作效率。

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，提供知识库系统，可助力党政军企等客户内部宣传与学习，沉淀知识及经验，打造数智化宣传教育体系。

信源密信提供用户个性化的按需配置能力，支持设置单位组织架构显示的安全保密策略，支持用户标签管理，可为不同的用户设置不同的用户标签，支持管理员后台建群，支持用户单位个性化配置，如自定义界面、自定义主菜单名称等。

信源密信产品形态多样，支持灵活部署，满足用户不同应用场景，既可提供部署在私有云或本地服务器的软件版本，又可提供标准机架式软硬一体服务器，还可提供无需固定IP地址的超小迷你服务器等。

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，既能支持小程序、H5、原生应用的快速集成，还能通过底座快速开发全新的业务系统，在密信里发布的应用或以密信为底座开发的系统都会完美的继承即时通信功能，同时应用或业务系统也可以在自身业务逻辑里调用即时通信接口。通过信源密信提供的服务器端API可以实现新业务系统与密信的互联互通。通过客户端的SDK可以让第三方App应用快速集成即时通信能力。

此外，信源密信还提供了开发、开放接口，支持与多类型应用以及用户现有业务进行无缝集成，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。相比传统的独立建设、相互割裂的业务系统搭建方式，信源密信一体化通信平台提供了统一的办公门户、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，有效提升了工作人员的办公效率，改善了数字化办公体验。

2.4 信源密信具备AI扩展能力，打造智能化工作接口生态

密信AI能力平台，作为信源密信的智能化配套产品，集成了多种开放的互联网以及私有化部署的大语言模型能力。该平台不仅能够有效整合并管理用户对大语言模型的访问权限和使用权限，还能根据客户的具体需求，安全地对接第三方大语言模型，为前端应用提供强大支持。这一平台能够为政府机构和企事业单位带来更加智能化的办公体验和业务流程，全面提升信息系统的智能化水平，显著提升工作效率。

密信AI能力平台快速落地场景化应用的能力开始显现，实现在“AI知识库”、“装备质量AI应用”、“财达股市通APP”等场景化应用。密信AI能力平台已经接入了国内优秀的大模型AI产品，如百度文心一言、阿里通义千问、智谱ChatGLM、Kimi以及科大讯飞星火大模型等，进一步提升了信源密信在智能交互和信息处理方面的能力，为用户提供多样化的智能服务选择。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。这一合作将充分发挥北信源在终端安全管理领域的专业优势，结合中译语通在人工智能与大数据技术创新应用方面的优势，共同助力提高国防军事、国家安全领域的科技成果转化和产业化应用，推动新质生产力同新质战斗力高效融合，为国防科技创新发展提供有力支撑。

信源密信的客户主要面向于党政军、国央企事业单位，已经覆盖大型客户、中小型客户、团体组织以及特殊行业客户，现已成功应用于众多国家重点工程和项目中。信源密信针对不同客户的需求和应用模式给出了完善的解决方案，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。依托于信源密信底座，结合实际行业及项目需求，信源密信打造了丰富的衍生品及可持续运营的解决方案：

（1）应急响应平台是北信源在《国家网络安全应急预案》等一系列政策的指引下，在国家重要部委的应急处置总体规划指导下，基于信源密信打造的应急响应解决方案。目前这套解决方案已经应用于网络安全应急响应平台、工控安全应急通信系统等。未来公司将抓住“十五五”全国应急体系建设规划机遇，加速推进网络安全应急指挥体系建设。

（2）智慧党建安全平台是针对基层党建工作的特殊性和实际需求，紧密围绕“四位一体”核心概念，重点开展基层党组织建设，定制一体化智慧党建解决方案。该平台以“信源密信”框架为基础，辅以安全体系（体系性）为重要保障，将党建工作与实际业务相结合（业务性），发挥极强的信息安全连通及互动能力（连通性），增进信息交互，同时对党建数据进行安全保护（安全性）。

（3）好家好社区智慧平台是基于5G/6G、物联网、AI、互联网+、智能终端技术，结合智慧社区建设需求，融合安防、物业服务、火灾预防、应急管理等系统建立的开放式的服务管理平台，实现小区内全方位软硬件设施的智能控制、数据采集与整合和综合管理，从而提升发现问题、解决问题的能力。

（4）市值分析管理系统是公司基于高效可靠、灵活可信的信息基础设施，专为上市公司实控人、大股东、董事会、证券事务部门打造的智能化市值分析管理系统。该系统具有上市公司市值分析管理、大股东减持/质押计算、上市公司线上视频会议、安全即时通信、移动办公通信等特色功能，可自动生成市值分析报告，科学打造成本分析可视化、财务规划科学化、工作安全沟通即时化，高效提高资本市场市值管理水平，进一步推动资本市场市值健康有序发展。

（5）中央网信办：公司配合国家网络安全法发布、协调保障党和国家各部委及关键信息设施网络安全，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网络平台，服务于中央、各地网信办、中央党政机关、网络安全应急办公室、人民团体、中央企业等机构，为实时掌握应急工作全局、应急处置提供强有力支撑。

（6）公安部：全国各系统在新一代移动警务网的基础上建设互联互通的即时通信平台。该平台现已经成功在湖北、甘肃、河南、江西、湖南等省部署使用，并完成全国80%以上的省与省之间互联互通。

（7）财政部：项目覆盖全国财政系统，整个系统部署在业务专网支撑财政体系的即时沟通，群组交流，适用于信创环境，实现了不同级别人员查看不同范围组织机构人员的使用需求。

（8）海南省：按照党中央国务院的决策部署，以信息化、智能化为支撑，加快推进社会管理信息化平台建设，努力推动社会治理体系和治理能力更上新台阶，海南省社会化治理平台项目采用北信源即时通信开发框架开发，集群化部署，集成了大量省内业务系统，为全面提升海南自贸区（港）的社会管理能力，实现“一线放开、二线高效管住”目标，为自贸区（港）建设保驾护航。

（9）国科智造APP：是某关键技术观察站联合北信源共同开发的高安全的国防工业大型产业链线上对接平台，于2022年珠海航展上发布；拥有四大核心功能：信息实时发布、专家权威评估、线上加密通信、全方位配套服务。国科智造APP突破了“民参军”信息壁垒和机制障碍，构建了先进技术产品军事应用的绿色通道。

公司组建了高水平的区块链团队，依托信源密信，展开了数据存证、健康医疗、社区管理等方面的应用研发。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，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的客户，被相关单位选为“指定安全通信平台”。荣获首批“办公即时通信软件安全能力”最高安全级别“卓越级”认证。报告期内首批获得“涉密信息系统”产品检测证书。已成为国家重要单位、重点工程、国家重要会议活动优选的即时通信平台和底座，装机量达千万台，深受行业用户好评。

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，传统防御手段亟需向智能化、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”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，当某区域温度异常升高时，系统自动触发防火门闭合指令，并联动消防栓启动，形成“感知-隔离-处置”闭环。

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，杜绝数据泄露风险。

2）智能设备协同管理：信源密信平台集成灭火器、消防水带、紧急照明等设备状态数据，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。

3.2 流程智能化：重塑军队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，推动军队管理向数字化、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。

多级审批流转：通过区块链技术固化审批流程节点，确保组织部门、管理人员、培训人员的权责透明可追溯。

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，实现灭火器、无人机反制设备等物资的全生命周期管理。例如，系统可自动监测消防栓压力状态，并在库存不足时触发采购流程，确保战备资源始终处于最佳状态。

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：在边境哨所、野外营地等场景部署边缘节点，实现本地化数据处理与低延时响应。

AI+区块链：利用区块链技术固化安防日志与审批记录，确保数据不可篡改；AI模型持续优化防御策略，提升系统自学习能力。

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：利用即时通信的实时交互能力，构建虚拟训练空间。士兵可通过VR设备参与多兵种联合模拟演练，指挥员实时调整战术方案，加速实战能力生成。

智慧军营建设：整合通信系统与智能安防、能源管理、后勤保障模块，打造“一屏统览、一网通办”的数字化军营生态，全面提升军队日常管理与战备水平。

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露。

动态权限分级：根据人员职级、任务属性动态调整通信权限。例如，战略级指挥员可通过“一人一密”通道下达指令，普通士兵仅限接收执行层任务信息，从源头杜绝越权访问风险。

区块链存证追溯：所有通信记录上链存储，结合时间戳与数字签名技术，确保信息不可篡改、操作全程可追溯。在军事审计或纠纷处理中，可快速调取完整通信链路，提升问责效率。

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：内嵌智能语义分析引擎，自动提取通信内容中的关键信息（如时间、坐标、装备需求），并生成结构化任务清单。例如，当收到“A区域需增派3辆装甲车”的语音指令时，系统自动触发资源调度流程，同步推送至后勤部门。

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。

智能会议管理：支持语音转写、多语种实时翻译、会议纪要自动生成等功能。在跨国联合军演中，不同语言参会者的发言可即时转化为文字并翻译，提升沟通效率与决策精准度。

移动化办公终端：适配军用加固平板、单兵智能终端等设备，支持离线加密通信与断点续传。在野外作战或信号屏蔽区域，士兵仍可通过本地Mesh网络实现小队间安全通信，确保指令不间断下达。

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，当遭遇网络攻击或电磁干扰时，系统自动切换至抗干扰通信频段，并启动备用卫星链路，保障关键指令的优先传输。

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。

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，以“信息之源，信任之源，信心之源，信念之源”为理念，秉承“为中国的数字化腾飞保驾护航”的企业使命，将“成为中国最值得信任的安全企业”作为企业愿景，坚持“内部崇尚奋斗、崇尚创新、崇尚实干；外部追求信任、追求专业、追求卓越”的价值观，以保障信息安全为己任，以人为本、开拓创新、追求卓越，牢牢巩固终端安全市场地位，全力打造安全即时通信龙头。

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。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，信源密信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