

► **信息支援部队建立再度凸显军工 IT 安全与大安全重要性。**随着国际形式不确定性增大，信息战频发，网络安全的重要性凸显。在此背景下，2024年4月19日，中国人民解放军信息支援部队成立大会在北京八一大楼隆重举行，国防部新闻发言人吴谦表示，调整组建信息支援部队，是党中央和中央军委从强军事事业全局出发作出的重大决策，是构建新型军兵种结构布局、完善中国特色现代军事力量体系的战略举措，对加快国防和军队现代化、有效履行新时代人民军队使命任务具有重大而深远的意义。信息支援部队是全新打造的战略性兵种，是统筹网络信息体系建设运用的关键支撑，在推动我军高质量发展和打赢现代战争中地位重要、责任重大。

► **网安军工 IT 如火如荼，新型体系稳步推进。**信息支援部队的建立为网络安全带来新的发展体系。其中：

► **1) 网络空间地图领域属于国家网络空间安全战略的核心组件，是海陆空天之外的第五空间的“底图”，**重要意义包括：实时感知智慧城市建设和运营情况，提高数字资产的管理效率；绘制数字政府全景图，为政府数字化转型提供技术支持；对工业互联网资产监控管理，保障工业互联网行业的安全稳定发展；通过对网络空间地形地貌的研究，对网络空间发生的安全问题进行精准预警和修复；构建病毒和漏洞传播影像图和漏洞修复图，实时追踪高风险漏洞影响程度及漏洞修复；突发紧急安全事件时，快速进行风险资产定位，并评估风险影响范围；进行网络攻防对抗中沙盘推演，通过绘制网络战场环境提高网络安全综合防控能力。

► **2) 网络靶场则是保障网络安全的重要基础设施。卫星加密赋予网络安全新的发展方向，有望成为全新增量，**卫星加密系统作用包括：可以在链路层对卫星通信系统实施加密保护，配合通信体制，解决终端入网认证、链路安全防护、全网密钥分发等技术难题；解决了卫星组播加密问题，保障视频会议、视频监控、组播业务、以及卫星自身的组播控制信令等大量组播业务安全稳定持续运行；中心站密码机、小站密码机、加密模块都可以实现透明部署，不改变现有网络结构，小站密码机支持无 IP 化部署模式，加电即插即用；中心站不受单台设备性能所限，可以无限叠加设备提升中心站加密链路接入能力，小站连接数量可以随着中心站叠加进行无限扩展。

► **行业领军公司加速落地产品体系。**盛邦安全拟收购天御云安，通过网络空间地图与卫星传输的组合进军卫星互联网安全领域。永信至诚发布“数字风洞”新品，开启数据安全“证无”新时代。安博通基于网络安全平台 SPOS 拓展网络安全产品，建立综合网安体系。普天科技通过公网通信和专网通信，推进卫星互联网产业发展。梅安森参股子公司获通信业务牌照，布局卫星互联网行业。

► **投资建议：**不确定性增长的国际地缘政治，凸显军工 IT 安全与大安全重要性。中国信息支援部队的建立实现了统筹国内网络信息体系建设运用的关键支撑，我国新型网络安全体系正在稳步推进，国家网络空间安全战略的核心组件网络空间地图与军工及重点单位虚拟训练基地网络靶场等美国近年来大力发展的新型特种网络安全产品有望快速发展，同时卫星传输加密或成为卫星互联网刚需并构建全新业务增量，建议关注普天科技、盛邦安全、梅安森、吉大正元、超图软件、中国长城、永信至诚、安博通等前瞻布局相关业务的厂商。

► **风险提示：**政策落地不及预期，技术发展不及预期。

推荐

维持评级



分析师 吕伟

执业证书：S0100521110003

邮箱：lvwei\_yj@mszq.com

## 相关研究

- 1.计算机周报 20240518: 较具弹性的地产链计算机公司-2024/05/18
- 2.计算机周报 20240512: 终端 AI 与国产化“东风”: 华为鸿蒙与国产算力全面崛起-2024/05/12
- 3.计算机周报 20240505: 2023 年年报与 2024 年一季报总结: 复苏中分化显著-2024/05/05
- 4.计算机周报 20240428: 再次强调国内算力需求或是最确定主线-2024/04/28
- 5.计算机行业点评: 密码产业或是量子产业最先落地应用-2024/04/27

# 目录

<b>1 信息支援部队建立再度凸显军工 IT 安全与大安全重要性</b>	<b>3</b>
1.1 国际形式加剧，信息安全成为兵家必争之地	3
1.2 我国成立首个信息支援部队叠加政策频发，凸显大安全重要性	4
1.3 卫星互联网安全技术变革	5
<b>2 军工 IT 如火如荼，新型体系稳步推进</b>	<b>6</b>
2.1 网络安全全新体系正逐步构建	6
2.2 卫星加密赋予网络安全新发展机遇	9
<b>3 行业领军公司加速落地产品体系</b>	<b>10</b>
3.1 普天科技：公网通信和专网通信齐发力，推进卫星互联网业务发展	10
3.2 盛邦安全：网络空间地图+卫星安全加密传输	10
3.3 梅安森：参股子公司获通信业务牌照，布局卫星互联网行业	11
3.4 吉大正元：军工军队业务持续推进	11
3.5 超图软件：GIS 领军者，特种应用方向逐步渗透	12
3.6 中国长城：前沿布局特种计算业务	12
3.7 永信至诚：网络靶场+数字风洞面向 AI 大模型安全测试	12
3.8 安博通：基于网络安全平台 SPOS 拓展网络安全产品	13
<b>4 投资建议</b>	<b>14</b>
<b>5 风险提示</b>	<b>15</b>
<b>插图目录</b>	<b>16</b>
<b>表格目录</b>	<b>16</b>

# 1 信息支援部队建立再度凸显军工 IT 安全与大安全重要性

## 1.1 国际形式加剧，信息安全成为兵家必争之地

**国际地缘持续对抗中，信息安全成为重中之重。**近年来，国际形式不确定性增大，俄乌战争、巴以冲突这类地区冲突引发世界环境动荡。而随着国际形式对抗加剧，网络空间的对抗日益频繁。据安全内参报道，俄乌战争期间，乌克兰的黑客组织攻击俄罗斯的军队、中央银行、油气公司等部门；而俄罗斯主要攻击目标为乌克兰政府和军队、国防工业企业、能源和电力等关键部门，网络空间已成为俄乌双方展开博弈和斗争的重要阵地。除了俄乌战争，近年其他的局部战争也都涉及到信息战的领域。

表1：信息战的实例

战争名称	信息战涉及组织	信息战如何进行
叙利亚战争	俄罗斯	电子战：用电子战武器破坏敌方通信系统； 心理战：利用社交媒体宣传恐怖组织暴行； 情报收集：与四国建立情报中心共享情报
俄乌冲突	北约	计算机网络作战：对俄罗斯进行网络攻击；心理战：利用社交媒体丑化俄罗斯的形象
伊拉克战争	美国	心理战：强化美国推翻萨达姆政权的正义性；通信保障：保护通信网络不被切断
巴以冲突	以色列、巴基斯坦	计算机网络作战：黑客组织攻击双方的网络基础设施； 心理战：双方在社交媒体推特、电报上展开舆论的博弈

资料来源：张冬青等《从伊拉克战争看信息化战争及信息战》，安全内参，民生证券研究院

**为了防范信息安全问题，各国与组织均将信息安全防护列为重点项目，相关组织与对应政策针对性频发。**而从美军的历次军事行动中，均能看见军事信息支援作战的重要性，其军事信息支援作战组织体系庞大，多军兵种部署，力量配属完备，作战流程设置清晰，可为各层级联合作战提供跨部门信息支援。

表2：各国的信息安全防护情况

国家与组织	信息安全相关组织	相关政策	信息安全项目
美国	国家安全委员会、国家安全局、 国防部、国土安全部	《2018 年 国 家 网 络 战 略》、 《国家网络安全战略实施计划》、 《2023 至 2025 年 CISA 战略规划》	“爱因斯坦”项目、“安全与弹性移动网络基础设施”计划、应急通讯计划、人工智能与机器学习战略计划
欧盟	欧盟网络安全局、 欧洲网络安全组织	《欧盟数字十年网络安全战略》、《网络安全战略的结论》、《网络安全法》	数字欧洲计划、“地平线欧洲”计划、CONCORDIA H2020 项目
俄罗斯	国家技术委员会、 俄罗斯数字发展部	《俄罗斯联邦国家安全战略》、 《信息、信息技术和信息保护》	俄罗斯联邦国家安全战略

资料来源：安全内参，民生证券研究院

**表3：美军信息支援部队组织架构**

组织层级	作用对象	组织架构
战略	政府部门、战区作战司令部或伙伴国 (组织)	国防部长, 分管政策的国防部副部长, 分管特种作战、低强度冲突、互通能力的助理国防部长, 国防部法律总顾问
战役	实施战区的政策或军事计划	联合参谋部、特种作战司令部司令、各军种部、各军种
战术	作战行动整体目标	军事信息支援作战特遣部(分)队

资料来源：彼德研究院微信公众号，民生证券研究院

## 1.2 我国成立首个信息支援部队叠加政策频发, 凸显大安全重要性

**信息支援部队作为全新打造的战略性兵种，是统筹网络信息体系建设运用的关键支撑。**在国际形式不确定性增大，信息战频发的背景下，2024年4月19日，中国人民解放军信息支援部队成立大会在北京八一大楼隆重举行，国防部新闻发言人吴谦表示，调整组建信息支援部队，是党中央和中央军委从强军事全局出发作出的重大决策，是构建新型军兵种结构布局、完善中国特色现代军事力量体系的战略举措，对加快国防和军队现代化、有效履行新时代人民军队使命任务具有重大而深远的意义。信息支援部队是全新打造的战略性兵种，是统筹网络信息体系建设运用的关键支撑，在推动我军高质量发展和打赢现代战争中地位重要、责任重大。

**除了信息支援部队的成立，近年来关于网络安全的政策法规热度不减。**从总书记在中央网络安全和信息化领导小组会议上第一次提出“没有网络安全就没有国家安全”以来，中央层面出台了一系列网络安全的政策法规，中国网络安全体系的“四梁八柱”逐渐形成。

**表4：网络安全相关政策法规**

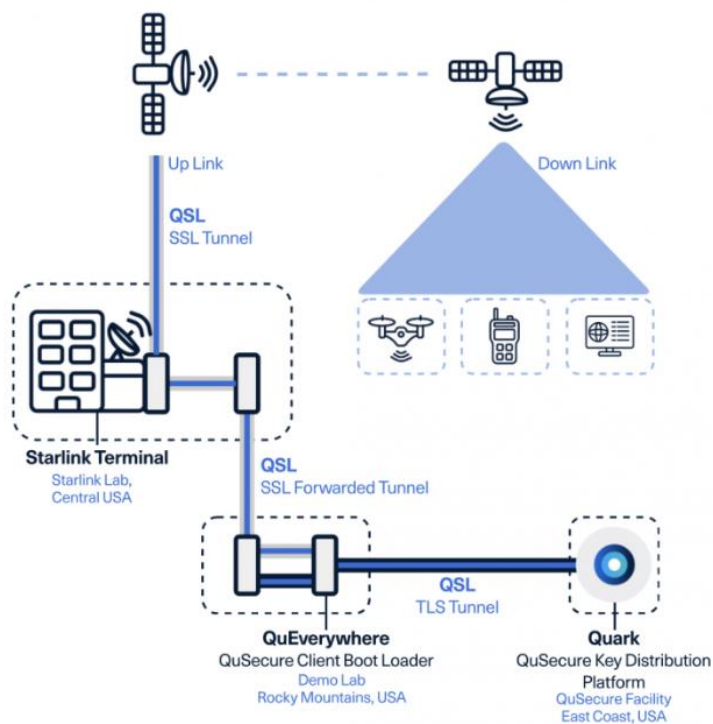
时间	政策法规名称	政策法规内容
2014年10月	《中共中央关于全面推进依法治国若干重大问题的决定》	加强互联网领域立法，完善网络信息服务、网络安全保护、网络社会管理等方面的法律法规
2017年6月	《中华人民共和国网络安全法》	申明了网络主权原则，建立了关键信息基础设施保护制度，成为我国网络空间法治化建设的重要里程碑
2021年4月	《关键信息基础设施安全保护条例》	内容包含关键信息基础设施认定、运营者责任义务、保障和促进、法律责任等
2021年6月	《中华人民共和国数据安全法》	聚焦于数据安全与发展、数据安全制度、数据安全保护义务以及政务数据开放与开放等内容
2021年12月	《网络安全审查办法》	对掌握超过100万用户个人信息的网络平台运营者赴国外上市增加了网络安全审查的项目

资料来源：中国教育和科研计算机网等，民生证券研究院整理

### 1.3 卫星互联网安全技术变革

实时端到端量子弹性加密通信链路提供数据保护。2023年3月9日，QuSecure公司与SpaceX合作，利用星链卫星实现了首个实时端到端量子弹性加密通信链路，这标志着美国卫星数据传输首次使用后量子密码技术，从而免受经典解密和量子解密攻击。QuSecure的解决方案是创建了一个安全的量子隧道，保护传输的数据免遭经典解密和抗量子解密，具体做法如下：首先，QuSecure通过上行链路将信号发送到星链卫星，然后通过下行链路发送回地球。而在数据传输过程中，量子安全层(QSL)保护所有传输中的数据。

图1: QuSecure 的卫星加密通信链路



资料来源：安全内参，民生证券研究院



## 2 军工 IT 如火如荼，新型体系稳步推进

### 2.1 网络安全全新体系正逐步构建

近年来，军工领域的网络安全体系受到各国重视，网络空间地图、网络靶场的建设形成浪潮。据安全内参、永信至诚官网：

1) 网络空间地图由网络空间测绘形成，美俄在二十世纪都形成了相关的军事计划。2006 年，美国国安局的藏宝图计划，以全网态势感知、侦察和攻击推演为目标，对网络空间进行多层次的信息探测和数据分析，形成大规模情报能力，探测内容包括：BGP、AS 和 IP 地址空间信息。2012 年，美国国防部国防高级研究计划局启动网络战发展项目“X 计划”，目的是生成网络空间作战态势图、制定作战方案、实施网络作战行动等。2014 年，俄罗斯卡巴斯基实验室发布网络威胁地图，致力于网络活动情况的实时表达。2015 年，美国国土局的 SHINE 计划，主要针对美国本土网络安全态势感知，建立美国本土网络空间关键基础设施信息数据库，监测关键行业网络可达性及安全态势，发现弱点设备和系统；

2) 作为支撑网络安全战略建设的重要基础设施，网络靶场正在成为世界各国抢先布局的网络作战新高地。美国早在 2008 年就启动“国家数位靶场”（NCR）计划，并于 2017 年启动持续网络训练环境（PCTE）建设，利用云端化平台方式满足分散各地、各军种网络作战部队的统一网络训练环境。

**应对网络安全的新体系，国内也迅速推进相关项目。**据安全内参、永信至诚，网络空间地图方面，2016 年，罗向阳等人在国内首次相对系统性地提出“网络空间测绘”一词，之后的学术研究都一致认为，网络空间测绘的目标是绘制一份网络空间地图。此后，相关公司发力网络空间地图相关领域，盛邦安全成为此领域的龙头企业。网络靶场方面，2021 年 7 月，工信部政策制定者呼吁政府和业界建设“AI 安全网络靶场”，促进网络靶场研究，利用网络靶场进行培训，并投资网络靶场，用于培训中国未来智慧城市的捍卫者。国内企业也相继发力，诞生了永信至诚这样的企业。从美国持续网络训练环境（PCTE）看国内网络靶场技术实践，国内网络靶场正在成长为网络强国建设的重要支撑。

**网络空间地图成为全新网络空间战略方向。**据盛邦安全招股书，网络空间地图领域属于国家网络空间安全战略的核心组件，是海陆空天之外的第五空间的“底图”，是网络空间的“高德地图”、“百度地图”。网络空间地图的重要意义体现在以下几个方面：1) 能实时感知智慧城市建设和运营情况，提高数字资产的管理效率；2) 绘制数字政府全景图，为政府数字化转型提供技术支撑；3) 对工业互联网资产监控管理，保障工业互联网行业的安全稳定发展；4) 通过对网络空间地形地貌的

研究，对网络空间发生的安全问题进行精准预警和修复；5) 构建病毒和漏洞传播影像图和漏洞修复图，实时追踪高风险漏洞影响程度及漏洞修复情况；6) 突发紧急安全事件时，能快速进行风险资产定位，并评估风险影响范围；7) 进行网络攻防对抗中的沙盘推演，通过绘制网络战场环境提高网络安全的综合防控能力。

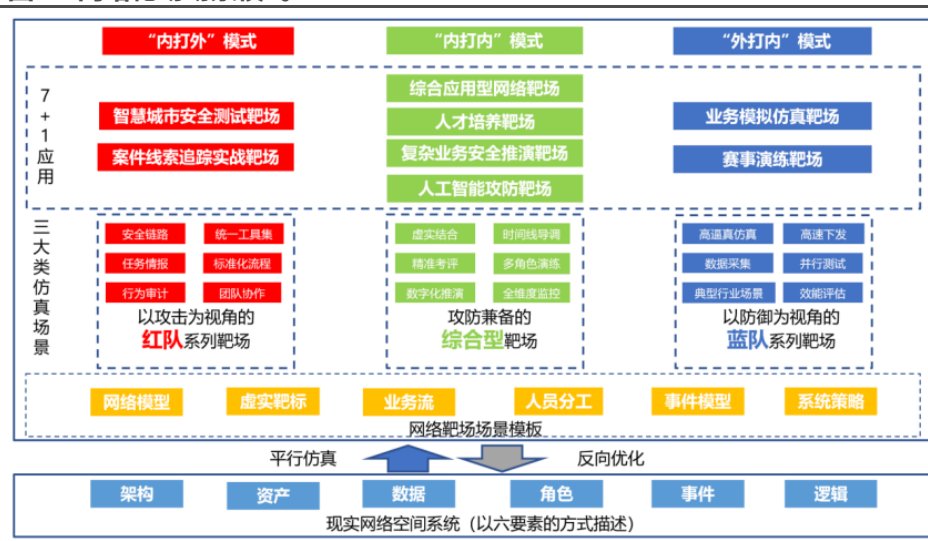
图2：网络空间地图的能力



资料来源：盛邦安全公众号，民生证券研究院

**网络靶场构建军工及重点单位虚拟训练基地。**据永信至诚 2023 年报，网络靶场是一种基于平行仿真技术，对真实网络空间中的网络架构、系统设备、业务流程的运行状态和运行环境，以及此环境中的行为和数据交互进行模拟、复现的技术或产品，以更有效地实现与网络安全相关的学习、科研、检验、竞赛、演习、推演、决策等行为，从而提高人员及机构的网络安全整体防护水平。网络靶场存在多种应用模式，既可以在靶场中模拟仿真各类高逼真的大规模场景用于进行实训演练或测试测评，也可以利用靶场作为统一的操作环境对外部网络进行实网演练和测试评估，或结合使用上述两种模式。其实质是客户利用网络靶场平台提供的虚拟化仿真场景、配套应用系统以及系列工具集来进行赛事演练、人才培养、智慧城市安全测试、案件线索追踪实战、业务模拟仿真、人工智能攻防、复杂业务安全推演等一种或多种业务活动的过程，作为网络空间的重要基础设施保障网络安全。近年来，勒索病毒、网络攻击、信息窃取等事件呈多发态势，我国面临的境外网络攻击和威胁越发严重，网络靶场也是保障网络安全的重要基础设施。

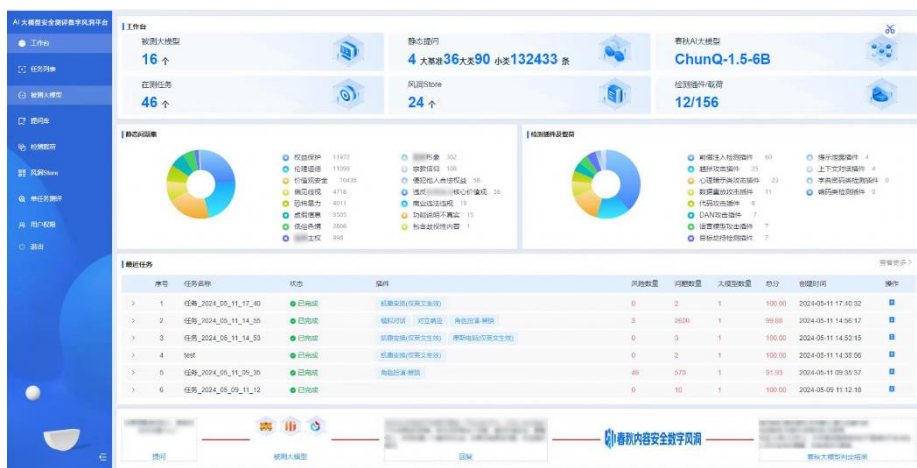
图3：网络靶场场景模式



资料来源：永信至诚招股书，民生证券研究院

**数字风洞脱颖而出，面向 AI+安全等全新场景。**据永信至诚 2023 年报，随着 AI 大模型广泛应用，潜在的安全风险也日益突出。数据泄露、模型篡改、内容价值观偏差等问题不断出现，引发社会各界对 AI 大模型安全的深切关注。AI 大模型亟需开展常态化测试评估，以保障 AI 数字健康。数字风洞的出现，帮助解决了 AI 大模型的安全问题。数字风洞是为数字化建设提供安全测试评估的基础设施，以“3×3×3×（产品×服务）”（第一个 3 指三类用户：城市、行业、单位；第二个 3 指三类场景：人、系统、数据；第三个 3 指业务周期的三个阶段：规划、运营、处置）安全感公式为方法论构建而成，通过在指定场景里对城市、行业、单位、人、系统、数据等各要素进行系统性风险验证，度量安全效果，提升综合防护能力。

图4：AI 大模型安全测评「数字风洞」平台



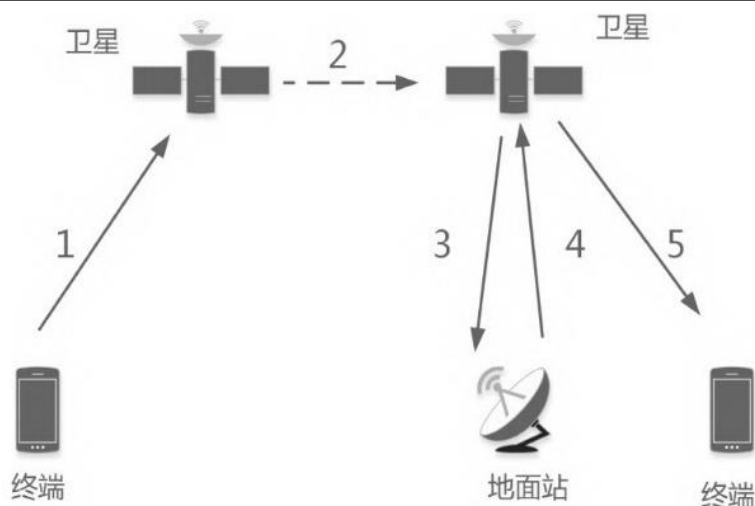
资料来源：永信至诚公众号，民生证券研究院



## 2.2 卫星加密赋予网络安全新发展机遇

**卫星信息传输方便快捷，但容易出现安全问题。**据左海等《“星链”安全设计理念初探》，卫星信息传输，是指地球上的两个或多个无线电通信站之间利用人造卫星作为中继站而进行的信息传输。在 SpaceX 的星链卫星中，卫星直接通过星间链路进行通信传输，包括处于同一轨道面上的卫星和处于相邻轨道面上的卫星。与传统的透明转发模式相比，星间链路的传输更快。但是，从网络安全视角看，攻击者可以从卫星终端、卫星、信关站、运行控制和运营支撑系统等多方位对星链系统实施攻击，同时还可以从供应链实施攻击，系统面临严峻的安全形势。

图5：星间链路传输模式



资料来源：左海等《“星链”安全设计理念初探》，民生证券研究院

**卫星通信加密为产业发展的构建安全基石。**据天御云安，卫星通信加密系统由主站密码机、小站密码机、密钥管理中心、配置管理中心四个部分组成。卫星通信加密系统提供了透明部署、高速加密、高带宽利用率的加密模式。支持卫星业务广播、业务组播以及流量分流等多种应用场景；保障卫星通信防探测、防窃密、防重放、防篡改。卫星加密系统的作用：1) 可以在链路层对卫星通信系统实施加密保护，配合通信体制，解决终端入网认证、链路安全防护、全网密钥分发等技术难题；2) 解决了卫星组播加密问题，保障视频会议、视频监控、组播业务、以及卫星自身的组播控制信令等大量组播业务安全稳定持续运行；3) 中心站密码机、小站密码机、加密模块都可以实现透明部署，不改变现有网络结构，小站密码机支持无 IP 化部署模式，加电即插即用；4) 中心站不受单台设备性能所限，可以无限叠加设备提升中心站加密链路接入能力，小站连接数量可以随着中心站叠加进行无限扩展。

### 3 行业领军公司加速落地产品体系

#### 3.1 普天科技：公网通信和专网通信齐发力，推进卫星互联网业务发展

在公网通信领域，公司聚焦网络领域规划、设计、优化、总承包等基础业务，以“5G+”技术和产品创新、横向多专业设计协同和纵向跨区域支撑管控，积极谋划布局卫星互联网产业的发展，在中国通信标准化协会（CCSA）参与了空、天、地多种模式下的协同组网的研究和标准制定工作，推进相关技术和产品研发。公司深入开展通信网络产品的研制并取得新突破，完成 5G 小基站、5G 直放站、5G 微分布等产品研制，实现 5G 小基站、5G 直放站、5G 微分布系统、5G 工业网关核心器件国产化。在专网通信领域，公司着力加快业务数字化、数据业务化，聚焦优势业务领域，推进智慧交通新基建，提升大数据服务能力和行业赋能效应。同时，积极推进空天地融合的面向应急等行业的专网通信应用。

#### 3.2 盛邦安全：网络空间地图+卫星安全加密传输

**网络空间地图叠加卫星安全加密传输，盛邦安全进军卫星互联网安全领域。**

2024 年 5 月 6 日，盛邦安全拟使用自有资金不超过人民币 3,000 万元持有天御云安不低于 60% 的股份，并与天御云安签署了《投资意向书》。盛邦安全在卫星互联网安全检测与防护技术方面的长期积累，结合天御云安在卫星通信加密行业的领先优势，将形成良好的产业协同效用。盛邦安全对天御云安的并购能够发挥两家公司的优点，进一步完成公司的战略升级目标，即卫星互联网安全业务。通过此次收购，公司将原有四大业务版块拓展至包括网络空间地图、身份安全、卫星互联网安全、密码安全、数据安全、云安全及安全服务的六大版块。此次收购完善了公司卫星互联网安全市场的战略布局，拓展了网络空间安全的覆盖范围，打开了公司未来新的成长曲线。

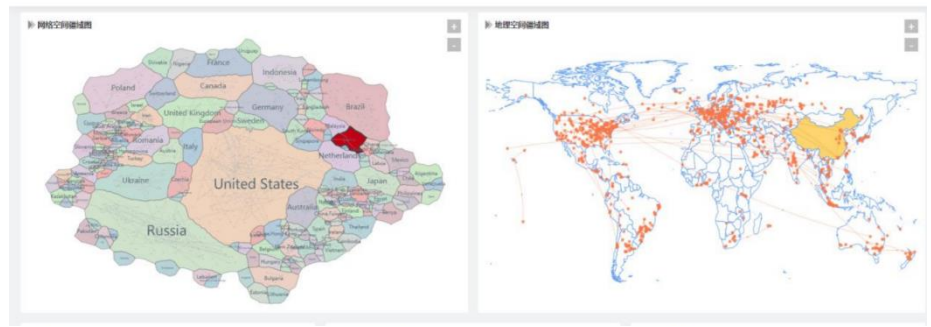
图6：天御云安的卫星通信加密系统部署



资料来源：天御云安官网，民生证券研究院

网络空间坤舆图，融合了盛邦安全在网络测绘、大数据分析、可视化等多个交叉领域的多年技术积累，通过主被动结合的探测手段，对网络空间环境进行“态”与“势”的多维度描绘，实现了网络空间与地理空间的关联与映射。网络空间地图领域将地理学、网络空间信息学、大数据、人工智能等诸多学科领域交叉融合，实现对网络空间疆域的治理功能，属于国家网络空间安全战略的核心组件。

**图7：盛邦安全的网络空间地图**



资料来源：盛邦安全招股书，民生证券研究院

### 3.3 梅安森：参股子公司获通信业务牌照，布局卫星互联网行业

2023年5月23日，梅安森宣布，参股公司重庆知与行物联科技有限公司获得由工业和信息化部颁发的面向全国范围的“国内甚小口径终端地球站通信业务”、“内容分发网络业务”以及“互联网接入服务领域的增值电信业务”经营许可证。目前，知与行推出的稀疏相控阵卫星通讯终端，可适配于汽车、特种车辆、各类船舶、单人背负、无人机、高铁等多种运动目标，同样也可适用于矿山、野外科考基地、石油钻井平台（陆地、海上）、家庭等可以固定安装的场景。此外，知与行推出的稀疏相控阵卫星通讯终端，即可满足与国内高轨卫星的宽带通信，由于采用相控阵体制，更可满足与低轨通信卫星的通信需求。

### 3.4 吉大正元：军工军队业务持续推进

公司为政府、军队以及金融、能源、电信、医疗、制造业等多个行业的企事业单位提供网络安全产品和服务，公司在军工军队方面持续推进型号项目研发及生产，并为中标新项目储备技术能力及资源。公司的产品与技术曾获得“国家科技进步二等奖”“2017年中国最具影响力软件和信息服务企业”“密码科学技术进步奖一等奖”“公安部科学技术一等奖”“教育部科技进步一等奖”“中国人民解放军科技进步二等奖”等重磅奖项。

### 3.5 超图软件：GIS 领军者，特种应用方向逐步渗透

GIS 是特种领域应用的核心技术支撑之一，目前公司在该领域的部分业务方向是领先供应商。2023 年公司加大第二增长曲线业务投入和市场开拓，特种领域取得了较好的成绩。目前 GIS 基础软件竞争格局清晰，大型商用 GIS 基础软件厂商主要为超图软件与美国供应商，GIS 基础软件管理数据较为敏感，关系国家安全，未来公司在特种领域前景广阔。

### 3.6 中国长城：前沿布局特种计算业务

公司系统装备业务中包含特种计算业务。公司聚焦国产关键软硬件生态体系，整合特种计算机业务资源和力量，努力成为主流的特种计算产品和信息化系统骨干提供商，系统装备业务实现重要突破，中标军办集采、天通同步一体设备等重大项目。同时，在海洋信息化方面，公司从事光纤水听器声纳分系统研制和业务拓展，涵盖水下探测、水下通信用光纤声纳核心产品，以及安全监测用分布式光纤传感监测装备，产品技术在业界领先。

### 3.7 永信至诚：网络靶场+数字风洞面向 AI 大模型安全测试

网络靶场历经多年发展，永信至诚已成领军者。春秋云境网络靶场平台基于永信至诚多年研发实践的平行仿真技术体系构建而成，该平台融合了主机虚拟化、网络虚拟化、软件定义网络、多维数据采集、3D 展示引擎和高可用云端架构等多种前沿技术，支持多种角色以不同权限和资源访问能力在同一靶场场景中进行联合交互和测试。

图8：永信至诚的网络靶场应用场景

网络靶场“7+1”应用场景



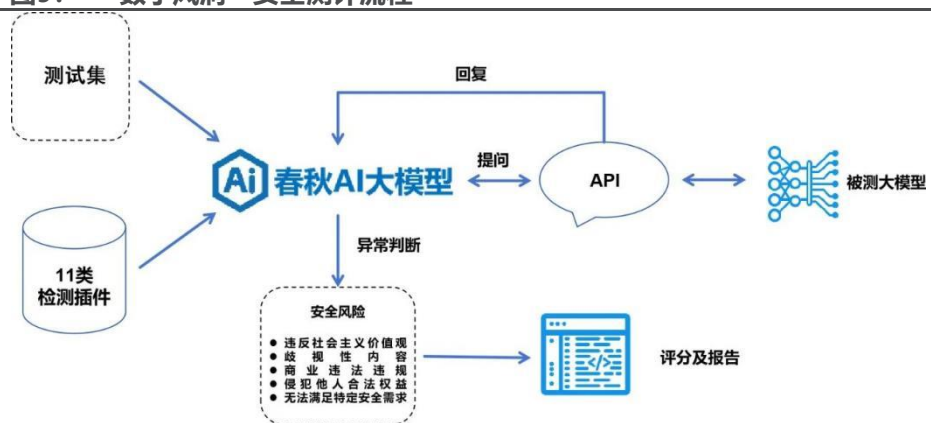
资料来源：永信至诚官网，民生证券研究院



“数字风洞”新产品发布，永信至诚开启数据安全“证无”新时代。在“形式合规”转向“实质合规”的行业背景下，永信至诚正式推出数据安全“数字风洞”产品，开启网络和数据安全由“证有”走向“证无”的新时代。”数字风洞“站在用户视角构建覆盖数据收集、存储、使用、加工、传输、提供、公开等全周期数据处理活动的测试评估体系，围绕数据安全业务、数据安全风险、威胁、合规等需求，化解数据安全治理挑战，解锁数据安全能力建设新发力点，提升数据安全工作成效。数字风洞的核心创新点是“风洞载荷时光机”子系统，该系统能够对测试环境和配套的测试风险载荷以“风洞时光”的形态进行封存，作为下一次测试的基础。每次测试前，系统都会优先将上一次风洞时光封存下来的风险载荷进行测试并验证，以确保之前发现的风险已经被成功消除，从而验证系统迭代优化后的成效。

“数字风洞”内容安全测评体系：1) 异常提问直接检测：以具有异常引导内容的原始提问测试集为基础，直接进行针对性安全检测；2) 提问变异检测：分别利用了 11 种针对 AI 大模型价值观对齐的检测方法进行变异生成新的提问，使用不同的测评插件及载荷对被测 AI 大模型发起提问；3) 表现异常判定：检查其回复是否存在异常内容，对异常数据进行标注；4) 内容安全评分：基于风险的重要性，「数字风洞」平台自动进行综合评估后打分。目前，“数字风洞”平台已接入百度千帆、通义千问、月之暗面、虎博、商汤日日新、讯飞星火、360 智脑、抖音云雀、紫东太初、孟子、智谱、百川等 20 余个 AI 大模型 API，以及 2 个本地搭建的开源 AI 大模型。

图9：“数字风洞”安全测评流程



资料来源：永信至诚公众号，民生证券研究院

### 3.8 安博通：基于网络安全平台 SPOS 拓展网络安全产品

以 SPOS 为基础，建立综合网安体系。SPOS 网络安全系统平台是安博通可

可视化网络安全技术的能力集，涵盖了安全控制、防御、检测、监测、审计、溯源等各阶段的关键技术引擎与特征库，提供了安全数据分析与学习的核心算法。平台具备灵活的嵌入性与开放性，可以与各类网络硬件融合，支持被第三方软件系统调用。公司以 ABT SPOS 平台为基础，形成了一系列网络安全产品，应用于网络安全防御控制、网络监测预警等领域，主要包括安全网关产品和安全管理产品两大类。

图10: SPOS 网络安全系统平台架构



资料来源：安博通官网，民生证券研究院

## 4 投资建议

不确定性增长的国际地缘政治，凸显军工IT安全与大安全重要性。中国信息支援部队的建立实现了统筹国内网络信息体系建设运用的关键支撑，我国新型网络安全体系正在稳步推进，国家网络空间安全战略的核心组件网络空间地图与军工及重点单位虚拟训练基地网络靶场等美国近年来大力发展的新型特种网络安全产品有望快速发展，同时卫星传输加密或成为卫星互联网刚需并构建全新业务增量，建议关注普天科技、盛邦安全、梅安森、吉大正元、超图软件、中国长城、永信至诚、安博通等前瞻布局相关业务的厂商。

## 5 风险提示

**1) 政策落地不及预期。**现阶段军工信息化与卫星互联网产业发展以政策驱动为主，若政策落地不及预期，或对相关公司的收入产生不利影响。

**2) 技术发展不及预期。**现阶段军工信息化项目如网络安全地图、网络靶场，已经卫星互联网加密技术均属较为复杂的前沿技术，若相关公司不能保持足够技术竞争力，或丢失订单并对收入产生不利影响。

## 插图目录

图 1: QuSecure 的卫星加密通信链路 .....	5
图 2: 网络空间地图的能力 .....	7
图 3: 网络靶场场景模式 .....	8
图 4: AI 大模型安全测评「数字风洞」平台 .....	8
图 5: 星间链路传输模式 .....	9
图 6: 天御云安的卫星通信加密系统部署 .....	10
图 7: 盛邦安全的网络空间地图 .....	11
图 8: 永信至诚的网络靶场应用场景 .....	12
图 9: “数字风洞”安全测评流程 .....	13
图 10: SPOS 网络安全系统平台架构 .....	14

## 表格目录

表 1: 信息战的实例 .....	3
表 2: 各国的信息安全防护情况 .....	3
表 3: 美军信息支援部队组织架构 .....	4
表 4: 网络安全相关政策法规 .....	4



## 分析师承诺

本报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并登记为注册分析师，基于认真审慎的工作态度、专业严谨的研究方法与分析逻辑得出研究结论，独立、客观地出具本报告，并对本报告的内容和观点负责。本报告清晰地反映了研究人员的研究观点，结论不受任何第三方的授意、影响，研究人员不曾因、不因、也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

## 评级说明

投资建议评级标准	评级	说明
以报告发布日后的 12 个月内公司股价（或行业指数）相对同期基准指数的涨跌幅为基准。其中：A 股以沪深 300 指数为基准；新三板以三板成指或三板做市指数为基准；港股以恒生指数为基准；美股以纳斯达克综合指数或标普 500 指数为基准。	推荐	相对基准指数涨幅 15%以上
	谨慎推荐	相对基准指数涨幅 5% ~ 15%之间
	中性	相对基准指数涨幅-5% ~ 5%之间
	回避	相对基准指数跌幅 5%以上
行业评级	推荐	相对基准指数涨幅 5%以上
	中性	相对基准指数涨幅-5% ~ 5%之间
	回避	相对基准指数跌幅 5%以上

## 免责声明

民生证券股份有限公司（以下简称“本公司”）具有中国证监会许可的证券投资咨询业务资格。

本报告仅供本公司境内客户使用。本公司不会因接收人收到本报告而视其为客户。本报告仅为参考之用，并不构成对客户的投资建议，不应被视为买卖任何证券、金融工具的要约或要约邀请。本报告所包含的观点及建议并未考虑个别客户的特殊状况、目标或需要，客户应当充分考虑自身特定状况，不应单纯依靠本报告所载的内容而取代个人的独立判断。在任何情况下，本公司不对任何人因使用本报告中的任何内容而导致的任何可能的损失负任何责任。

本报告是基于已公开信息撰写，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、意见及预测仅反映本公司于发布本报告当日的判断，且预测方法及结果存在一定程度局限性。在不同时期，本公司可发出与本报告所刊载的意见、预测不一致的报告，但本公司没有义务和责任及时更新本报告所涉及的内容并通知客户。

在法律允许的情况下，本公司及其附属机构可能持有报告中提及的公司所发行证券的头寸并进行交易，也可能为这些公司提供或正在争取提供投资银行、财务顾问、咨询服务等相关服务，本公司的员工可能担任本报告所提及的公司的董事。客户应充分考虑可能存在的利益冲突，勿将本报告作为投资决策的唯一参考依据。

若本公司以外的金融机构发送本报告，则由该金融机构独自为此发送行为负责。该机构的客户应联系该机构以交易本报告提及的证券或要求获悉更详细的信息。本报告不构成本公司向发送本报告金融机构之客户提供的投资建议。本公司不会因任何机构或个人从其他机构获得本报告而将其视为本公司客户。

本报告的版权仅归本公司所有，未经书面许可，任何机构或个人不得以任何形式、任何目的进行翻版、转载、发表、篡改或引用。所有在本报告中使用的商标、服务标识及标记，除非另有说明，均为本公司的商标、服务标识及标记。本公司版权所有并保留一切权利。

## 民生证券研究院：

上海：上海市浦东新区浦明路 8 号财富金融广场 1 幢 5F； 200120

北京：北京市东城区建国门内大街 28 号民生金融中心 A 座 18 层； 100005

深圳：广东省深圳市福田区益田路 6001 号太平金融大厦 32 层 05 单元； 518026