



北京永信至诚科技股份有限公司

（北京市海淀区丰豪东路 9 号院 6 号楼 103）

关于北京永信至诚科技股份有限公司 首次公开发行股票并在科创板上市申请文件 审核问询函的回复

保荐机构（主承销商）



国信证券股份有限公司
GUOSEN SECURITIES CO.,LTD.

（深圳市罗湖区红岭中路 1012 号国信证券大厦十六层至二十六层）

上海证券交易所：

贵所于 2021 年 7 月 27 日出具的《关于北京永信至诚科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》（上证科审（审核）（2021）471 号）（以下简称“审核问询函”）已收悉。北京永信至诚科技股份有限公司（以下简称“永信至诚”“发行人”“公司”）与国信证券股份有限公司（以下简称“保荐机构”）、北京济和律师事务所（以下简称“发行人律师”）、天健会计师事务所（特殊普通合伙）（以下简称“申报会计师”）等相关方对审核问询函所列问题进行了逐项核查，现回复如下，请审核。

如无特别说明，本问询函回复使用的简称与《北京永信至诚科技股份有限公司首次公开发行股票并在科创板上市招股说明书（申报稿）》（以下简称“招股说明书”或“《招股说明书（申报稿）》”）中的释义相同。

审核问询函所列问题	黑体（不加粗）
审核问询函所列问题答复	宋体
对招股说明书的修改与补充	楷体（加粗）

注：本问询函回复部分表格中单项数据加总数与表格合计数可能存在微小差异，这些差异均因计算过程中的四舍五入形成。

目录

目录.....	3
1、关于科创属性.....	4
2、关于主营业务.....	33
3、关于网络安全科技馆建设项目	88
4、关于行业竞争情况及同行业公司对比.....	145
5、关于业务资质.....	159
6、关于采购和供应商.....	170
7、关于集成商.....	176
8、关于收入.....	186
9、关于期间费用.....	215
10、关于应收账款.....	226
11、关于存货.....	244
12、关于现金流量.....	253
13、关于其他.....	260
14、保荐机构总体意见.....	279

1、关于科创属性

根据申报材料：（1）发行人是专注网络靶场和网络安全人才培养的软件企业；（2）公司主要产品及服务包括网络靶场与人才培养、安全管控与蜜罐、安全工具类产品、安全防护系列服务和网络安全竞赛服务；除“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0APT 安全监测产品（增强级）”产品外，发行人其他产品不属于计算机信息系统安全专用产品，亦不属于“网络关键设备和网络安全专用产品目录”所列示的范围；（3）公司属于新一代信息技术行业，符合科创属性评价标准一；公司取得 8 项授权发明专利，其中 6 项与核心技术相对应，公司主营业务均使用到了公司的核心技术；公司最近三年营业收入复合增长率为 27.11%。

请发行人说明：

（1）结合国家科技创新战略规划、行业领域相关规划或相关细分领域规划、政策及其具体内容，进一步论证发行人作为专注网络靶场和网络安全人才培养的软件企业，其相关产品或服务符合国家科技创新战略要求的具体依据；（2）结合报告期内“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0APT 安全监测产品（增强级）”两项产品的销售情况及除上述两项产品外，发行人其他产品均不属于计算机信息系统安全专用产品，亦不属于“网络关键设备和网络安全专用产品目录”所列示范围的情况，进一步论证发行人认定其产品为网络安全产品的依据是否充分；发行人主要产品或服务与《战略性新兴产业重点产品和服务指导目录（2016 年版）》中新一代信息技术行业的对应情况；发行人的业务实质是软件还是系统集成；（3）6 项发明专利在核心技术中发挥的具体作用，发行人核心技术先进性的具体体现；结合核心技术在相关产品或服务中的具体应用情况，论证公司主营产品或服务均使用到相关核心技术的依据；（4）结合在手订单及业绩预计情况等，说明发行人是否持续符合科创属性评价指标。

请保荐机构、发行人律师对上述事项以及发行人是否符合与科创板定位相关的科创属性要求进行核查，并发表明确意见。

【回复】

请发行人说明：

（1）结合国家科技创新战略规划、行业领域相关规划或相关细分领域规划、

政策及其具体内容,进一步论证发行人作为专注网络靶场和网络安全人才培养的软件企业,其相关产品或服务符合国家科技创新战略要求的具体依据;

永信至诚是一家聚焦科技创新的网络安全企业,是国家级专精特新“小巨人”企业,核心业务为网络靶场系列产品。网络靶场是数字化建设过程中安全性测试的重要基础设施,是检验和评估安全防御体系有效性的关键技术系统,是国家对重大网络安全风险和趋势进行推演和论证研判的重要科学装置,是防范化解重大网络安全风险的重要手段,也是政企、院校、科研机构等单位网络安全人才培养的重要支撑平台。

国际上,网络靶场同样是网络安全保障的重要基础设施,美国、英国、德国、俄罗斯、日本和韩国等国家积极进行网络靶场的建设。其中,美国 2008 年启动的国家网络靶场(NCR)定位于“涵盖测试、训练、研究、验证等”“能够真实的重现人类行为和弱点”“复现大规模军用网络和政府网络的能力”“所有能够发射和接收数字信息的系统必须进行网络空间安全测试”等重要方向。

公司的网络靶场应用场景广泛,其中一项应用场景是人才培养靶场,人才培养靶场通常以软硬件一体的方式部署在用户的网络环境中,成为其人才培养、训练、选拔、评价的重要基础平台。公司所指人才培养主要并非授课培训,报告期内公司线上线下培训收入占比较低,分别为 5.39%、6.51%、3.24%和 3.97%。公司的核心业务围绕网络靶场进行,已在多个领域发挥重要作用,符合国家科技创新战略要求。

一、国家战略方面

根据《国家中长期科学和技术发展规划纲要(2006—2020 年)》《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》等与国家科技创新战略相关的文件,公司符合国家科技创新战略相关的情况如下表:

文件名称	发文单位	主要相关内容	公司业务情况
国家中长期科学和技术发展规划纲要(2006—2020 年)	国务院	1、信息产业及现代服务业 以发展高可信网络为重点,开发网络信息安全技术及相关产品,建立信息安全技术保障体系,具备防范各种信息安全突发事件的技术能力。 2、面向核心应用的信息安全 重点研究开发国家基础信息网络和重要信息系统中的安全保障技术,开发复杂大系统下	网络靶场是网络安全保障技术的重要基础。公司主要产品为以网络靶场为核心的网络安全产品和网络安全服务。

		的网络生存、主动实时防护、安全存储、网络病毒防范、恶意攻击防范、网络信任体系与新的密码技术等。	
国务院关于印发“十三五”国家科技创新规划的通知	国务院	第七章 发展保障国家安全和战略利益的技术体系 四、发展维护国家安全和支撑反恐的关键技术 强化科技对国家应对传统安全和非传统安全紧迫需求的支撑，支持信息安全、网络安全、生物安全、反恐、保密等方面关键核心技术研发。	公司产品和服务主要面向信息安全、网络安全方向。
国家创新驱动发展战略纲要	国务院	四、战略任务 (一) 推动产业技术体系创新，创造发展新优势 1. 发展新一代信息技术，增强经济社会发展的信息化基础。加强类人智能、自然交互与虚拟现实、微电子与光电子等技术研究，推动宽带移动互联网、云计算、物联网、大数据、高性能计算、移动智能终端等技术研发和综合应用，加大集成电路、工业控制等自主软硬件产品和网络安全技术攻关和推广力度，为我国经济转型升级和维护国家网络安全提供保障。	公司通过持续研发投入，形成平行仿真和网络攻防两大类核心技术，公司产品和服务所处行业为网络安全行业，公司核心技术属于网络安全技术。
中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要	国务院	第十八章 营造良好数字生态 第三节 加强网络安全保护 健全国家网络安全法律法规和制度标准，加强重要领域数据资源、重要网络和信息系统安全保障。建立健全关键信息基础设施保护体系，提升安全防护和维护政治安全能力。加强网络安全风险评估和审查。加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力。加强网络安全关键技术研发，加快人工智能安全技术创新，提升网络安全产业综合竞争力。加强网络安全宣传教育和人才培养。	公司网络靶场可用于关键信息基础设施保护体系，并用于网络安全风险评估、人才培养、人工智能安全技术创新等领域。安全管控与蜜罐产品符合“提升威胁发现、监测预警、应急指挥、攻击溯源能力”的要求。

二、行业分类方面

发行人所属行业为国家战略性新兴产业，公司产品符合《战略性新兴产业重点产品和服务指导目录（2016 版）》《战略性新兴产业分类（2018）》要求，具体如下：

文件名称	发文单位	所属分类	公司业务情况
战略性新兴产业重点产品和服务指导目录（2016 版）	国家发改委	1、（2.4.2 网络与信息安全软件）支撑系统安全保障及业务应用安全的风险评估、安全测评等网络与信息安全支撑类软件产品等	1、公司的网络靶场系列产品是用于支撑系统安全保障及业务应用安全的风险评估、安全测评等网络与信息安全支撑类软件产品；

		2、（2.4.2 网络与信息安全软件）统一威胁管理平台软件、网络行为监控软件等网络与边界安全类软件产品 3、（2.4.3 网络与信息安全服务）网络违法信息监测发现、定位管理系统，网络违法行为追踪定位、取证系统等违法信息及行为的监测管理类产品 4、（2.4.3 网络与信息安全服务）网络与信息安全咨询服务、网络与信息安全运行维护服务、网络与信息安全风险评估、信息系统等级保护咨询等 5、（2.4.3 网络与信息安全服务）网络与信息安全培训、网络与信息安全教育培训等	2、公司的安全管控与蜜罐产品属于统一威胁管理平台软件、网络行为监控软件等网络与边界安全类软件产品； 3、公司的安全工具类产品属于网络违法信息监测发现、定位管理系统，网络违法行为追踪定位、取证系统等违法信息及行为的监测管理类产品； 4、公司的安全防护系列服务属于网络与信息安全咨询服务、网络与信息安全运行维护服务、网络与信息安全风险评估、信息系统等级保护咨询等； 5、公司的网络安全竞赛服务和其他服务属于网络与信息安全培训、网络与信息安全教育培训等。
战略性新兴产业分类（2018）	国家统计局	1.3.2 网络与信息安全软件开发之 6519 其他软件开发之网络安全软件和专用安全软件	公司产品和服务所处行业为网络安全行业，公司主要业务为网络安全软件开发。

三、行业细分方面

从行业细分方面，公司细分行业及主要产品符合《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》《关于加强网络安全学科建设和人才培养的意见》、各省数字政府建设等内容，具体如下：

文件名称	发文单位	主要相关内容	公司业务情况
网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）	工信部	“一、总体要求”之“（三）发展目标”：人才培养。建成一批网络安全人才实训基地、公共服务平台和实训靶场，创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人才规模质量不断提高 “二、重点任务”之“6.加强共性基础支撑”：加快发展源代码分析、组件成分分析等软件供应链安全工具，提升网络安全产品安全开发水平。积极推进网络靶场技术研究，建设结合虚拟环境和真实设备的安全孪生试验床，提升网络安全技术产品测试验证能力。	公司核心业务为网络靶场，研究网络靶场技术，符合行动计划中的重点方向。 公司网络靶场系列产品之一“人工智能攻防靶场”属于行动计划中的人工智能安全靶场。该靶场用于人工智能网络攻防对抗可行性、可用性研究验证。在特定范围内为人工智能的安全攻防机器人生成训练环境和测试数据集，形成了人工智能二进制漏洞挖掘利用和

		“二、重点任务”之“专栏1”：研究人工智能系统可解释性、隐私性等安全要素，突破人工智能模型攻击与防御关键技术，设计实现人工智能系统自动攻防平台，构建人工智能安全靶场。 “二、重点任务”之“专栏2”：打造网络安全“靶场云”，建设数字孪生靶场，为城市安全能力验证等提供支撑。构建网络安全“服务云”，聚集智慧城市安全规划、建设、运营等服务资源，保障城市安全有序运行。	防御、多级复杂网络场景的综合渗透等多种模式的AI训练评估靶场，为AI技术从实验室模型向实战应用转化提供了必备的科研及验证环境。
关于加强网络安全学科建设和人才培养的意见	中央网信办	“八、完善网络安全人才培养配套措施”：人才是网络安全第一资源。各地方、各部门要认识到网络安全学科建设和人才培养的极端重要性，增强责任感使命感，将网络安全人才培养工作提到重要议事日程。根据本意见精神，结合实际制定具体措施，支持网络安全学院学科专业建设，加快网络安全人才培养，为实施网络强国战略、维护国家网络安全提供强大的人才保障。	公司网络靶场系列产品之一“人才培养靶场”用于支撑高校等网络空间安全教学和实训，服务于人才培养。 同时，公司还提供了网络安全人才培训服务，设计了“知识讲解-实验模拟-在线测试-效能评估”的整套网络安全实训体系，积极构建了“培训-选拔-认证-输送四位一体，线上线下相结合”的实战型网络安全人才培养体系，为学习者提供有效成长路径。
国家能源局关于加强电力行业网络安全工作的指导意见（国能发安全〔2018〕72号）	国家能源局	“五、加强行业网络安全基础设施建设”之“（十五）建设网络安全仿真验证环境”：适应电力行业网络安全研究、测试、演练等应用需求，整合现有资源，建立覆盖发、输、变、配、用、调度全环节的网络安全仿真验证环境，开展重大网络安全事件模拟验证、漏洞挖掘、攻防演练、业务培训等工作。建设行业网络安全重点实验室。	在能源行业，网络安全仿真验证环境即靶场。 公司网络靶场系列产品之一“业务模拟仿真靶场”和“复杂业务安全推演靶场”用于重大网络安全事件模拟验证、漏洞挖掘、攻防演练、业务培训等工作。
关于印发2021年电力安全监管重点任务的通知（国能综通安全〔2021〕12号）		“三、重点任务”之“（六）加强电力生产安全监管”：加强电网及网络安全监管。强化并网电厂涉网安全监管和电力重大设备安全监管，开展重要输电通道风险隐患排查，建立联防联控机制，实施风险管控和挂牌督办。加强对煤矿、机场等重要用户的用电安全监管。推进电力行业网络安全仿真验证环境（靶场）建设，组织开展电力行业网络安全攻防实战演练。	公司网络靶场系列产品之一“业务模拟仿真靶场”和“复杂业务安全推演靶场”用于网络安全仿真验证环境（靶场）建设。
广东省数字	广东省人	将结合安全大数据和安全应用，打造	公司核心业务为网络靶

政府改革建设“十四五”规划（粤府〔2021〕44号）	民政府	安全攻防实验室，构建网络安全仿真靶场与实训环境，持续开展“粤盾”攻防演练，提升数字政府整体安全实战能力。	场，研究网络靶场技术，符合各省数字经济中的重点方向。
浙江省数字经济五年倍增计划（浙政办发〔2018〕91号）	浙江省人民政府	推进网络攻防演练工程。定期举办网络安全攻防演练大赛和网络安全比赛，加强技术交流。建设攻防实验室，搭建网络安全攻防靶场、模拟仿真环境，开展教学、实训、渗透攻击测试、研究以及专业培训。	
广西数字经济发展规划（2018-2025年）（桂政发〔2018〕39号）	广西壮族自治区人民政府	建设大数据安全靶场，开展大数据与网络攻防演练。推动合同、发票、证据、档案、凭证等电子化转变，加快构建安全可信的数字商务运行环境。	

四、国家实验室操作方面

鹏城实验室是中央批准成立的突破型、引领型、平台型一体化的网络通信领域新型科研机构，作为国家战略科技力量的重要组成部分，以网络通信、网络空间和网络智能为主要研究方向，开展领域内战略性、前瞻性、基础性重大科学问题和关键核心技术研究。

鹏城实验室首批 5 个科研项目为未来区域网络试验与应用环境、南海立体通信网络示范验证平台、云脑开源平台与智能应用、网络技术仿真验证平台、自主可控生态环境。

网络技术仿真验证平台即鹏城网络靶场，鹏城网络靶场在互联网仿真平台方面突破了系列关键技术，在目标网络规模（百万级节点）及其灵活部署，网络安全事件准确检测（有效性到 90%以上），网络实验任务并发数（1000 个实验并发）等方面达到了世界领先水平。

发行人与各大高校、企业作为鹏城网络靶场的分靶场，支持鹏城网络靶场的建设工作，如下：



五、专精特新“小巨人”方面

公司 2021 年被遴选为国家级专精特新“小巨人”，具备较强的技术实力。

文件名称	发文单位	内容
《关于支持“专精特新”中小企业高质量发展的通知》（财建〔2021〕2 号）	财政部、工业和信息化部	2021-2025 年，中央财政累计安排 100 亿元以上奖补资金，引导地方完善扶持政策和公共服务体系，分三批（每批不超过三年）重点支持 1000 余家国家级专精特新“小巨人”企业（以下简称重点“小巨人”企业）高质量发展，促进这些企业发挥示范作用，并通过支持部分国家（或省级）中小企业公共服务示范平台（以下简称公共服务示范平台）强化服务水平，聚集资金、人才和技术等资源，带动 1 万家左右中小企业成长为国家级专精特新“小巨人”企业。
关于开展第三批专精特新“小巨人”企业培育工作的通知（工信厅企业函〔2021〕79 号）	工业和信息化部	为“十四五”期间培育百万家创新型中小企业、十万家省级“专精特新”中小企业、万家专精特新“小巨人”企业打下坚实基础，为推动经济高质量发展、构建新发展格局提供有力支撑。
中共中央政治局会议	-	要强化科技创新和产业链供应链韧性，加强基础研究，推动应用研究，开展补链强链专项行动，加快解决“卡脖子”难题，发展专精特新中小企业。

综上所述，公司是一家聚焦科技创新的网络安全企业，是国家级专精特新“小巨人”企业，核心业务为网络靶场系列产品。公司的网络靶场系列产品、安全管控与蜜罐产品、网络安全竞赛等产品和服务符合《国家中长期科学和技术发展规划纲要（2006—2020 年）》《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》等与国家科技创新战略相关的文件和要求；符

合《战略性新兴产业重点产品和服务指导目录（2016 版）》《战略性新兴产业分类（2018）》分类要求。公司产品和服务符合行业发展重点方向，是鹏城网络靶场的组成部分，符合各省数字经济的重点方向，符合国家科技创新战略要求。

（2）结合报告期内“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0APT 安全监测产品（增强级）”两项产品的销售情况及除上述两项产品外，发行人其他产品均不属于计算机信息系统安全专用产品，亦不属于“网络关键设备和网络安全专用产品目录”所列示范围的情况，进一步论证发行人认定其产品为网络安全产品的依据是否充分；发行人主要产品或服务与《战略性新兴产业重点产品和服务指导目录（2016 年版）》中新一代信息技术行业的对应情况；发行人的业务实质是软件还是系统集成；

一、发行人产品为网络安全产品

（一）“春秋云阵蜜罐系统”和“慧眼高级威胁检测系统 V2.0APT 安全监测产品（增强级）”的销售情况

除上述两项销售许可证外，公司安全可视化日志分析平台于 2021 年 7 月 8 日取得《计算机信息系统安全专用产品销售许可证》，公司共有 3 个产品销售许可证，如下所示：

序号	证书编号	产品名称	核发部门	有效期至
1	0108201163	慧眼高级威胁检测系统 S1-V2.0APT 安全监测产品（增强级）	公安部网络安全保卫局	2022.8.15
2	0503201087	春秋云阵蜜罐系统 ECQYZ-HA/V2.0 主机型入侵检测产品（基本级）		2022.8.8
3	0405211221	计算机信息系统安全专用产品销售许可证-安全可视化日志分析平台 ECQ-TSGZ-A100/V1.0 日志分析（一级）		2023.7.8

公司销售具有产品销售许可证的产品收入报告期内占比较低，不足 5%，主要是蜜罐产品和工具类产品，而公司营业收入的主要来源为发行人的网络靶场系列产品。网络靶场属于网络安全建设的重要基础设施，目前国内网络靶场市场正处于起步阶段，主管部门暂未要求具备相关配套资质。

发行人的网络安全产品除以上已取得《计算机信息系统安全专用产品销售许可证》外，发行人其余网络安全产品是不同分类标准下的网络安全产品，该等产品同样针对网络安全场景，用于解决网络安全问题，但因技术特征或产品功能不同，未被列入计算机信息系统安全专用产品类型和《网络关键设备和网络安全专

用产品目录（第一批）》（“第一批名录”）范围。

和同行业上市公司相比，像启明星辰、安恒信息、奇安信等产品范围涵盖防火墙、入侵检测等标准网络安全产品的公司，销售许可证数量较多，可达数十个甚至上百个，同行业上市公司美亚柏科产品包括网络空间安全产品，主要客户为网络安全监管部门、军队等，其产品亦未包含防火墙、入侵检测等标准产品，其销售许可证为3个，分别为幽荧网络威胁预警系统、破冰光安全数据单向传输系统、光安全数据单向传输系统。与公司较为相近。

（二）《网络关键设备和网络安全专用产品名录》与网络安全产品

“第一批名录”的范围小于市场上网络安全产品类型的范围。

目前，虽然没有权威的官方机构对网络安全产品及服务进行分类，但各研究机构对网络安全行业分类大同小异。根据中国信息通讯研究院发布的《网络与信息安全产业白皮书（2015年）》的分类，网络安全产品包括防火墙、入侵检测和防御、统一威胁管理、安全内容管理、安全评测工具、终端安全管理、身份管理与访问控制、安全平台和其他安全产品。

第一批名录于2017年6月1日公布施行，该名录所列设备和产品主要为网络关键设备和网络安全专用产品，只是网络安全产品中的一部分。第一批名录主要目的是加强对进入名录中产品的监管及检测，内容如下所示：

大类	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量（双向） $\geq 12\text{Tbps}$ ；整系统路由表容量 ≥ 55 万条
	2. 交换机	整系统吞吐量（双向） $\geq 30\text{Tbps}$ ；整系统包转发率 $\geq 10\text{Gpps}$
	3. 服务器（机架式）	CPU数量 ≥ 8 个；单CPU内核数 ≥ 14 个；内存容量 $\geq 256\text{GB}$
	4. 可编程逻辑控制器（PLC设备）	控制器指令执行时间 ≤ 0.08 微秒
网络安全专用产品	5. 数据备份一体机	备份容量 $\geq 20\text{T}$ ；备份速度 $\geq 60\text{MB/s}$ ；备份时间间隔 ≤ 1 小时
	6. 防火墙（硬件）	整机吞吐量 $\geq 80\text{Gbps}$ ；最大并发连接数 ≥ 300 万；每秒新建连接数 ≥ 25 万
	7. WEB应用防火墙（WAF）	整机应用吞吐量 $\geq 6\text{Gbps}$ ；最大HTTP并发连接数 ≥ 200 万
	8. 入侵检测系统（IDS）	满检速率 $\geq 15\text{Gbps}$ ；最大并发连接数 ≥ 500 万
	9. 入侵防御系统（IPS）	满检速率 $\geq 20\text{Gbps}$ ；最大并发连接数 ≥ 500 万
	10. 安全隔离与信息交换产品（网闸）	吞吐量 $\geq 1\text{Gbps}$ ；系统延时 $\leq 5\text{ms}$

11. 反垃圾邮件产品	连接处理速率(连接/秒)>100; 平均延迟时间<100ms
12. 网络综合审计系统	抓包速度≥5Gbps; 记录事件能力≥5万条/秒
13. 网络脆弱性扫描产品	最大并行扫描IP数量≥60个
14. 安全数据库系统	TPC-EtpsE (每秒可交易数量) ≥4500个
15. 网站恢复产品(硬件)	恢复时间≤2ms; 站点的最长路径≥10级

由上表可见, 第一批名录中的网络安全专用产品主要为防火墙、IDS、IPS等传统的网络安全专用产品, 并未涵盖全部的网络安全产品。

发行人的网络安全产品因技术特征不同、产品形态不同等原因暂未被列入第一批名录, 因此未取得网络关键设备和网络安全专用产品安全认证证书, 但主要用途仍是用于网络安全相关的场景。

(三) 《计算机信息系统安全专用产品》与网络安全产品

计算机信息系统安全专用产品的范围小于网络安全产品的范围。

计算机信息系统安全专用产品的范围和分类详见本回复“5、关于业务资质”之“(3)除“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0APT 安全监测产品(增强级)”产品外, 发行人其他产品均无需办理《计算机信息系统安全专用产品销售许可证》的依据, 是否符合相关法规要求和行业惯例”之“二、《计算机信息系统安全专用产品销售许可证》的适用范围”之“(一)计算机信息系统安全专用产品的范围”。

计算机信息系统安全专用产品主要系用于保护计算机信息系统安全的专用硬件和软件(防御性的硬件和软件), 未涵盖所有的网络安全产品。除取得《计算机信息系统安全专用产品销售许可证》的网络安全产品外, 发行人还研发了可用于攻防演练、业务支撑和安全辅助等场景的多种网络安全产品。

二、发行人主要产品或服务与《战略性新兴产业重点产品和服务指导目录(2016年版)》中新一代信息技术行业的对应情况

具体详见本回复“1、关于科创属性”之“(1)结合国家科技创新战略规划、行业领域相关规划或相关细分领域规划、政策及其具体内容, 进一步论证发行人作为专注网络靶场和网络安全人才培养的软件企业, 其相关产品或服务符合国家科技创新战略要求的具体依据”。

三、发行人的业务实质为软件而非系统集成

发行人的业务实质是以自主研发的软件为主的产品及服务, 而非系统集成。

从产品性质上看，参考原《计算机信息系统集成资质管理办法（试行）》的规定，计算机信息系统集成是指从事计算机应用系统工程和网络系统工程的总体策划、设计、开发、实施、服务及保障；根据《计算机软件保护条例》的规定，计算机软件是指计算机程序及其有关文档，其中，计算机程序，是指为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可以被自动转换成代码化指令序列的符号化指令序列或者符号化语句序列；文档，是指用来描述程序的内容、组成、设计、功能规格、开发情况、测试结果及使用方法的所有文字资料和图表等。发行人的业务实质为软件而非计算机信息系统集成。

从产品形态上看，发行人的主要产品为网络靶场系列产品、安全管控与蜜罐产品和安全工具类产品，该等产品的形态分为软件和软硬件一体化两种形态。其中，后者的生产流程为采购相应的硬件产品，进行组装调试，然后将自主研发的软件或采购的软件及系统灌装入硬件设备中。发行人的软件产品对硬件的依赖程度较低，硬件通常是作为软件的载体，未达到系统集成的程度。

从产品毛利率上看，发行人主营业务毛利率分别为 67.54%、66.69%、56.40%、56.77%。根据公开披露信息，上市公司东华软件股份公司系统集成业务 2020 年的毛利率为 10.61%，太极计算机股份有限公司系统集成业务 2020 年的毛利率为 13.16%，新晨科技股份有限公司系统集成业务 2020 年的毛利率为 10.94%，荣联科技集团股份有限公司系统集成业务 2020 年的毛利率为 5.14%，系统集成行业整体毛利率较低；上市公司中国软件与技术服务股份有限公司自主软件产品业务 2020 年的毛利率为 74.55%，用友网络科技股份有限公司软件及云服务业务 2020 年的毛利率为 59.9%，北京华宇软件股份有限公司应用软件 2020 年的毛利率为 54.80%。发行人报告期内的毛利率与上市公司软件产品业务的毛利率水平接近，且远高于一般上市公司系统集成业务的毛利率，原因在于发行人的业务实质为软件，该等软件产品主要由发行人自主研发，因此毛利率水平较高。

发行人毛利率与同行业上市公司启明星辰、美亚柏科、绿盟科技、深信服、安恒信息、安博通、山石网科、奇安信毛利率平均水平相近，同行业上市公司分类如下：

序号	公司名称	证监会行业	东财行业
1	启明星辰	信息传输、软件和信息技术服务业	其他软件服务

2	美亚柏科	信息传输、软件和信息技术服务业	其他软件服务
3	绿盟科技	信息传输、软件和信息技术服务业	行业应用软件
4	深信服	信息传输、软件和信息技术服务业	行业应用软件
5	安恒信息	信息传输、软件和信息技术服务业	其他软件服务
6	安博通	信息传输、软件和信息技术服务业	行业应用软件
7	山石网科	信息传输、软件和信息技术服务业	其他软件服务
8	奇安信	信息传输、软件和信息技术服务业	其他软件服务

由上表可见，同行业上市公司行业分类均为软件行业。

发行人各项主要产品和服务的实质情况具体如下：

类别	发行人主要产品	业务实质
网络靶场系列产品	春秋云境网络靶场平台	软件和硬件一体化产品
安全管控与蜜罐产品	春秋云阵新一代蜜罐系统	软件产品
	春秋云势网络安全态势感知与处置平台	软件产品
安全工具类产品	流量监测、数据分析、业务支撑、安全辅助类产品	软件产品
安全防护系列服务	安全检测与评估、安全咨询、安全运维与分析处置、安全能力建设与评估等服务	服务
网络安全竞赛服务	网鼎杯、强网杯、护网杯、巅峰极客等网络安全大赛	服务
其他服务	线上安全培训、线下安全培训	服务

此外，作为软件企业，发行人已根据《国务院关于印发新时期促进集成电路产业和软件产业高质量发展若干政策的通知》《中华人民共和国工业和信息化部、国家发展改革委、财政部、国家税务总局公告 2021 年第 10 号》和《国家发展改革委等五部门关于做好享受税收优惠政策的集成电路企业或项目、软件企业清单制定工作有关要求的通知》（发改高技[2021]413 号）等规定取得了《国家鼓励的重点软件企业》资质。

综上，发行人的业务实质为软件而非系统集成。

（3）6 项发明专利在核心技术中发挥的具体作用，发行人核心技术先进性的具体体现；结合核心技术在相关产品或服务中的具体应用情况，论证公司主营产品或服务均使用到相关核心技术的依据；

一、6 项发明专利在核心技术中发挥的具体作用

截至 2021 年 6 月 30 日，公司获得授权发明专利为 8 项，在审发明专利 8 项，

合计 16 项。截至本回复出具日，公司获得授权发明专利 9 项，新增城市级网络靶场的 VLAN 划分方法和系统获得授权，在审发明专利 7 项，合计 16 项，获得授权的发明专利中有 7 项与公司核心技术密切相关，具体如下：

序号	专利名称	密切相关的核心技术
1	一种木马行为识别方法与系统	恶意代码检测分析技术
2	一种关联搜索方法和系统	基于镜像差分压缩和分级存储的节点快速重构技术、分布式存储及深度分析技术
3	信息搜索与发布方法与系统	-
4	一种对等网络应用的监控方法与系统	基于可扩展元场景的复杂业务模拟技术、基于对抗的非接触高精度溯源反制框架技术
5	一种基于动态字典的视频播放方法与系统	-
6	一种信息安全竞赛的管理系统及管理方法	面向平行仿真的高性能靶场平台搭建与服务技术、基于可扩展元场景的复杂业务模拟技术
7	一种云平台虚拟资源高速调度方法与系统	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于镜像差分压缩和分级存储的节点快速重构技术、高性能动态可配置的容器服务承载集群技术
8	一种网络靶场系统中的数据采集方法及数据采集系统	基于脆弱点感知的高甜度蜜罐构建技术、内核级攻击行为全景捕获与复现技术、面向应激反制的交互式对抗环境生成技术
9	城市级网络靶场的 VLAN 划分方法和系统	基于多重隔离的高并发异步靶场构建技术、面向应激反制的交互式对抗环境生成技术

注：上表中“信息搜索与发布方法与系统”“一种基于动态字典的视频播放方法与系统”两项专利亦用于公司主营业务，这两项专利对应的技术未列为核心技术。

发明专利在核心技术中的具体作用如下：

序号	核心技术名称	与专利及软著对应	重点解决的问题	发明专利在核心技术中发挥的具体作用
1	基于混合虚拟化的属性平行仿真技术	专利： ZL201611045951.6： 一种云平台虚拟资源高速调度方法与系统（原始取得）	网络安全仿真测试环境缺失问题	网络靶场作为进行人才实训、演练、方案验证以及科研研发和测试等业务的基础设施，需要能够快速高效的为业务提供高度仿真的实验环境。而在网络靶场行业内，场景的仿真度通常可以分为两个级别：场景网络架构及节点属性仿真、场景数据及行为仿真。 本核心技术主要解决网络安全仿真测试环境缺失问题中的场景网络架构及节点属性的仿真问题，根据场景的特点融合使用靶场机、容器、模拟器、程序仿真、实体设备等，用较低的成本采用软件定义的方式来描述、创建、存储、克隆以及销毁各类靶场场景。而专利“一种云平台虚拟资源高速调度方法与系统”则通过相关的技术将数台到数千台的常规服务器、网络设备、安全设备和特定的实验设备等组成云化的资源池进行统一的资源管理，利用本核心技术中的场景描述方式和场景复现仿真能

				力,实现了在同一套硬件基础设施上,可以进行各种各样规模、类型和复杂程度的构建下发和资源管理调度的平台系统。没有此专利技术的支持,本核心技术的平行仿真在实践中难以达到高效的实用价值。
2	基于靶场同步行为仿真技术	专利: ZL201611045951.6: 一种云平台虚拟资源高速调度方法与系统(原始取得)	网络安全仿真测试环境缺失问题	此核心技术主要解决网络安全仿真测试环境缺失问题中的数据和行为仿真的问题。 在真实的网络中,会存在有各类的背景数据流量、业务数据、网络使用者的各类网络行为等等,为了使网络场景不仅“长得像”,更要“有灵魂”,就需要使场景中能够根据需求按照策略,定期、随机或按某种算法不断的产生一些对应的数据或行为。专利“一种云平台虚拟资源高速调度方法与系统”则通过相关的技术将数台到数千台的常规服务器、网络设备、安全设备和特定的实验设备等组成云化的资源池进行统一的资源管理,利用本核心技术中的场景描述方式和场景复现仿真能力,实现了在同一套硬件基础设施上,可以进行各种各样规模、类型和复杂程度的构建下发和资源管理调度的平台系统。没有此专利技术的支持,本核心技术的平行仿真在实践中难以达到高效的实用价值。
3	面向高性能靶场平台搭建与服务技术	专利: ZL201611045951.6: 一种云平台虚拟资源高速调度方法与系统(原始取得)、 ZL201610624541.0: 一种信息安全竞赛的管理系统及管理方法(原始取得)	网络安全仿真测试环境缺失问题	靶场平台的搭建主要需要解决多个物理服务器、网络设备的统一资源管理问题,在每个计算节点、存储节点以及网络设备中均需部署相应的控制模块,靶场中心平台需实时了解各个物理节点上的资源的当前状况,并根据相应的保障算法将当前开机的靶场机分配到合理的计算节点上去,这个过程中需要对较为耗时的IO访问等进行稳定性和速度上的提升和保障。 专利“一种云平台虚拟资源高速调度方法与系统”所采用的方法是高性能靶场平台构建和服务的重要组成部分,是其实现的必备条件之一。用于网络竞赛是靶场的基本功能之一,竞赛赛前、赛中、赛后以及数据分析处理等相关技术的专利“一种信息安全竞赛的管理系统及管理方法”是本核心技术的重要部分之一,使核心技术能够满足网络安全竞赛对靶场平台的时效性、容错性和稳定性等苛刻要求。
4	基于可扩展场景复杂业务模拟技术	专利: ZL201310381658.7: 一种对等网络应用的监控方法与系统(原始取得)	网络安全仿真测试环境缺失问题	网络场景可以交换机为支撑节点划分为多个子网,而每一个子网或多个子网可以组成可扩展的元场景,多个元场景可以通过嵌套、组合、链接而形成更加复杂的场景,而为了能够快速将现实世界中的一个网络虚拟仿真到靶场中,就需要先对其进行扫描,自动化的留存和采集这个网络场景的重要数据,包括网络的拓扑架构、每个网元的IP、端口、操作系统、

		ZL201610624541.0: 一种信息安全竞赛的管理系统及管理方法(原始取得)		应用、服务信息、流量特征、人员行为等等,采集到的数据可以同靶场底层支持库中的相应数据进行对比关联,如果没有的,可以通过监控程序采用半人工方式予以补齐使其补充进靶场资源库中,从而在靶场中形成元场景,以场景模板形式为后期的使用打造基础,进行嵌套、扩展、复制组合等。 专利“一种对等网络应用的监控方法与系统”解决了从现有基础系统中进行数据监控采集和原型生成的问题,使复杂业务模拟的基础模板生成具有了自动化元素采集的可能。专利“一种信息安全竞赛的管理系统及管理方法”保证了竞赛或演练类场景的全过程数据留存。
5	基于镜像差分压缩和分级存储的节点快速重构技术	专利: ZL201310037074.X: 一种关联搜索方法和系统(原始取得)、ZL201611045951.6: 一种云平台虚拟资源高速调度方法与系统(原始取得)	网络安全仿真测试环境缺失问题	网络IO是云化的靶场平台在进行场景克隆的最大挑战,为了快速的在多个物理节点之间复制和传输大的靶场模板文件,因此对靶场模板进行了拆分,采用集中存储、本地多级存储等方式将大文件拆分成多个小块的方式进行多级缓存,保障了资源的快速调度和分发复制,是虚拟资源高速调度实现的基础技术之一。 专利“一种关联搜索方法和系统”解决了核心技术中在差分压缩镜像和分级存储后,在多个计算节点和存储节点以及集中存储节点中快速的查找到属于某一靶场模板或继承模板的多个文件分块的问题。专利“一种云平台虚拟资源高速调度方法与系统”则提供了将这些文件分块快速的进行资源克隆、传输以及整合的技术。
6	基于多重隔离的高并发靶场构建技术	专利: ZL201910435998.0: 城市级网络靶场的VLAN划分方法和系统(原始取得)	网络安全仿真测试环境缺失问题	在同一套网络靶场基础设施基础上,可以同时并发的执行多组实验任务,实验任务共享相应的计算资源、存储资源和网络资源,但基于靶场的隔离技术使得每个任务在资源层面上均与独立运行在一组完全物理隔离的实体资源上一样。专利“城市级网络靶场的VLAN划分方法和系统”是网络靶场进行网络虚拟化隔离的关键技术之一,通过此技术可以以软件定义的方式将策略快速下发给基础设施内的虚拟以及实体交换设备从而快速的划分隔离的网络资源以支持不同的任务使用,并可以快速回收动态使用。
7	基于脆弱点的敏感度蜜罐构建技术	专利: ZL201910557426.X: 一种网络靶场系统中的数据采集方法及数据采集系统	提升网络安全防御有效性问题	高甜度蜜罐构建需要解决的主要问题,是从蜜罐仿真或复现的网络场景上来讲,需要达到“以假乱真”的地步,即蜜罐中的场景需要同被部署位置的网络融为一体,并且有足够的特点和“诱饵”使攻击者认为这个蜜罐是有价值且脆弱,进而有利可图的。因此在特定的网络位置部署的蜜罐需要具备根据周围环境配置和改变自己网络空间特征以及脆弱性漏洞特征

		(原始取得)		的能力。本核心技术的价值就在于此。专利“一种网络靶场系统中的数据采集方法及数据采集系统”解决蜜罐系统在部署到相关网络位置后,快速的扫描和采集周边网络,获取网络特征和复制重要特征数据等问题。
8	内核级攻击全景与内网攻击复现技术	专利 : ZL201910557426.X : 一种网络靶场系统中的数据采集方法及数据采集系统 (原始取得)	提升网络安全防御有效性问题	本技术应用于靶场和蜜罐中,在靶场机或主机中对特定的行为、系统状态、关键系统信息的改变,文件、权限、服务的变化等等进行数据采集和复现。专利“一种网络靶场系统中的数据采集方法及数据采集系统”中实现的采集方法和系统是核心技术中捕获和复现部分的重要内容。
9	恶意代码检测分析技术	专利 : ZL201310381668.0: 一种木马行为识别方法与系统 (原始取得)	提升网络安全防御有效性问题	专利“一种木马行为识别方法与系统”为该核心技术的其中一个专有分类,主要针对木马类相关恶意代码的检测和发现。
10	高性能的动态配置容器承载技术	专利 : ZL201611045951.6: 一种云平台虚拟资源高速调度方法与系统 (原始取得)	提升网络安全防御有效性问题	本核心技术实现了在互联网的公有云资源池中快速的编排和配置相关容器实现靶场机资源的集群式部署和使用。核心技术使用了专利“一种云平台虚拟资源高速调度方法与系统”中的虚拟资源相关调度算法和实现方式,将其应用在公有云基础之上,实现了高性能和动态可配置的效果。
11	分布式存储及深度分析技术	专利 : ZL201310037074.X : 一种关联搜索方法和系统 (原始取得)	提升网络安全防御有效性问题	本核心技术主要用于组件分布式存储分析架构,实现分布式数据仓库、海量数据收集、数据总线、搜索引擎等组件,完成对海量信息数据的接入和处理分析。专利“一种关联搜索方法和系统”为关键技术的实现提供了高性能的数据搜索方法和关联分析算法等。
12	基于对抗的非接触高精度溯源反制框架技术	专利 : ZL201310381658.7: 一种对等网络应用的监控方法与系统	提升网络安全防御有效性问题	本核心技术用于实现高精度的反制溯源框架的开发,进行反制溯源需要首先完成攻击者各类攻击数据和行为的采集、识别和留存,并将这些行为特征和样本等与特征库、威胁情报库中的相关信息进行对比、碰撞和关联从而将其在攻击中留存下来的各类蛛丝马迹匹配得到其虚拟身份或真实身份。专利“一种对等网络

		(原始取得)		应用的监控方法与系统”在数据监控采集以及搜索碰撞部分提供技术支持。
--	--	--------	--	-----------------------------------

二、发行人核心技术先进性的具体体现

(一) 构建高逼真实战化网络靶场的核心技术

公司自主研发的基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术和基于可扩展元场景的复杂业务模拟技术,提升了产品的多种跨领域业务场景的高逼真仿真能力。相关核心技术先进性的具体体现如下:

序号	核心技术名称	核心技术说明	核心技术先进性的具体体现	对应的产品或服务
1	基于混合虚拟化的属性平行仿真技术	提出平行仿真环境中关键要素属性平行仿真方法,按照目标场景的架构特点和靶标属性,利用自动化方式对各级网络中的资产进行信息采集,记录每个靶标的操作系统、服务、应用、漏洞、协议及业务等相关信息和特征指纹,结合人工分析形成标准化描述报告和场景模板的蓝图。通过与靶场平台靶标库已保存的靶标模板进行关联和匹配,大幅度提升了仿真的逼真度,减少场景模板的构建时间和难度;利用靶标全虚拟化节点、轻量级虚拟化节点、离散事件模拟技术、程序化仿真节点、协议流量仿真节点和实物节点六种不同节点形态的混合虚拟化融合仿真,在节点中的任意两者之间均可进行组网和数据通信,提升了场景实例化过程中的资源利用率和下发效率;针对无法使用虚拟化或其他仿真方式进行高逼真仿真的实体设备,利用靶场的软件定义和动态调整虚拟网络的能力,将实体设备的管理端口和业务端口动态的接入各类实验场景和网络,保证靶场内的场景在特定的物理属性方面与目标场景保持高度的一致性,实现了虚拟设备和物理设备的混合组网,从而提升了属性平行仿真程度。	本技术将网络空间中的多种元素标准化和数据化,并采用特有的描述和存储方式,利用靶场云平台中的多种虚拟、仿真和模拟技术,将真实网络空间中的关键架构、节点、应用、脆弱性等靶场中予以复现,利用虚拟化技术替代真实网络中的实际物理设备,在保证逼真程度的情况下节约复现成本。且使用软件化模板方式进行存储,可进行反复的克隆、下发使用。	网络靶场系列产品、安全、管控与蜜罐产品、网络安全竞赛服务
2	基于靶标分层同步的行为平行仿真技术	高逼真的仿真一个目标场景不仅仅需要在网络架构、操作系统、应用、服务、漏洞等基础场景层面做到一致,还需要在场景中运行的数据、业务、行为也需保持活性和逼真性。在数据和业务仿真方面,采用分层数据流采集的模式,在目标网络中有针对性的对不同层次的数据流进行采集和留存,编制流量仿真重放策略,将这些有典型代表性的数据流在仿真场景中进行重放,赋予场景数据基础活力,进一步提升仿真效果;在行为模拟方面,利用自动化脚本的方式对网络应用行为、业务行为、攻击行为、安全运维行为、加固行为等进行描述,进一步的提升仿真效果并可以根据策略灵活配置,模拟出真实业务应用中各种常规行为,通过智能化程序能够按照通常的人类行为方式对这些行为进行模拟和重现,在靶场平台中将内置丰富的攻击模拟智能化程序,从而提升了整个攻防行为的逼真性。	本技术通过将网络流量、网元行为、人员操作行为、多种网元的状态变化、联动属性等进行数字化的统一留存和复现,达到实验环境与真实网络空间极为接近的行为特性。	网络靶场系列产品、安全、管控与蜜罐产品、网络安全竞赛服务

3	基于可扩展元场景的复杂业务模拟技术	针对大规模网络靶场业务复杂、节点众多、拓扑多样等特点，提出基于可扩展元场景的复杂业务模拟技术。提出基于最小元场景的多分区管理、多场景要素整合的复杂场景模型描述方法，解决了精准、高效描述复杂场景模型的难题。针对复杂场景模型节点众多难以扩展模拟的问题，采用了复杂业务场景结构描述文件记录的方法并采用元场景分区描述技术，针对性读取场景节点数据、结构数据或连通性数据，大幅提高读取效率。针对复杂网络的模拟难题，在场景描述文件的场景结构描述中引入了多重嵌套技术，将复杂网络拆解为小的典型结构，并支持小型场景作为一个子区域引入至主场景描述文件中，实现了以最小元场景为单位的复杂业务扩展模拟技术。利用该方法，解决了复杂业务场景下大规模靶场构建难、构建步骤繁杂以及本地存储瓶颈的难题，为大规模靶场构建提供了标准化描述体系和元场景扩展构建技术。	解决大型网络场景进行软件化描述的问题，将网络架构以网络设备网元为主干、终端网元为叶子节点构建成靶场场景图谱，实现场景的可扩展、可嵌套、可分布式开机，实现分区域、分布式的虚拟网络软件定义化管控。	网络靶场系列产品、安全、管控与蜜罐产品、网络安全竞赛服务
---	-------------------	---	--	------------------------------

（二）构建大规模高性能网络靶场的核心技术

面向平行仿真的高性能靶场平台搭建与服务技术、基于镜像差分压缩和分级存储的节点快速重构技术、基于多重隔离的高并发异步靶场构建技术和高性能动态可配置的容器服务承载集群技术，突破了复杂业务场景在建模、并发多任务克隆、场景实例化等方面存在时间消耗突出的关键难题，实现了在弹性基础设施上的大规模、高性能靶场构建能力。相关核心技术先进性的具体体现如下：

序号	核心技术名称	核心技术说明	核心技术先进性的具体体现	对应的产品或服务
1	面向平行仿真的高性能靶场平台搭建与服务技术	利用虚拟资源动态资源感知均衡调度技术，将云中心的资源调度过程分为三个阶段：资源初始分配、资源动态调度以及资源动态整合，通过主要应用靶场机迁移技术将负载过高的物理机上的靶场机迁移到资源利用率较低或者空闲物理机上，以此来实现负载均衡，并尽量减少服务等级协议冲突的概率；利用集约规划的虚拟资源分配技术，从软件即服务的角度实现在保证满足用户需求的前提下降低资源使用成本，将云平台中的虚拟资源分配问题进行建模，研发了基于本地节点效用和全局效用的决策模型，该模型的云平台由一组物理机组成，每个物理机通过虚拟化平台管理多个靶场机，实现靶场机可以在任意的两个物理机器之间进行迁移并利用监控技术对当前应用程序的性能进行监控，通过动态决策技术根据当前应用程序的负载和资源分配情况进行性能评估，从而决定是否需要分配更多的靶场机，还是释放空闲的靶场机。通过此模型的应用能够对靶场云计算环境中的虚拟资源进行高效的分配与管理，解决了在模拟仿真过程中云资源有效利用的问题。	采用统一的资源调度算法和管控模型，将数台到数千台计算和存储服务器以及实验用设备的资源进行实时监控和资源管理，最优化的选择空闲的物理节点来下发和克隆靶场机，对每个靶场机、模拟设备等的实际工况进行监控，遇到资源不足时灵活迁移靶场机实现业务的透明切换，保障靶场实验场景的稳定、顺畅使用。	网络靶场系列产品、安全、管控与蜜罐产品、网络安全竞赛服务

序号	核心技术名称	核心技术说明	核心技术先进性的具体体现	对应的产品或服务
		题。		
2	基于镜像差分压缩和分级存储的节点快速重构技术	针对大规模网络靶场存储性能差、节点实例化难度大、节点存储拥塞等特点，提出基于镜像差分压缩和分级存储的节点快速重构技术。为完成靶场机模板本地克隆、跨主机克隆等操作，实现靶场机文件无存储压力复制，设计了镜像差分压缩技术，实现主模板加增量模板的靶标模板体系，降低了存储网络的带宽拥塞可能性，实现计算节点优先派发，使节点具备高可用、动态水平扩展、动态垂直扩展、压力自适应等特性，实现多节点重构。为保证存储网络具有足够的带宽和充足的性能，提出了分级存储节点快速重构技术，将存储网络流量和其他类型的网络流量物理隔离，以保证存储网络的独立性和高效性。利用该方法，实现了繁琐任务并发执行，充分发挥镜像差分压缩和分级存储的优势，有效缩短场景构建时间，可实现基于节点重构的大规模靶场构建。	该技术解决复杂大规模场景在集中进行模板分发、克隆构建时对基础设施网络的IO集中峰值压力的问题，将大的靶场机模板文件分片成若干个较小的分片，并采用调度算法将常用的增量分片存储在多级存储网络中，充分调度全部网络资源共同分担集中下发的突发压力，提高分发效率保证分发质量，提升容错效果。	网络靶场系列产品、安全、管控与蜜罐产品、网络安全竞赛服务
3	基于多重隔离的高并发异步靶场构建技术	针对场景实例化难以保持稳定、高速，步骤繁琐以及时间消耗突出的问题，提出基于多重隔离的高并发异步靶场构建技术，将繁琐任务进行拆分并分散到不同的计算节点服务器上并发执行，提高了创建效率，缩短了场景构建时间。采用基于多重隔离的消息队列，将外部消耗服务器资源的同步请求转化为异步请求，并按消息种类进行划分并发执行；实现任务调度、任务执行、后端存储和任务自动发现，大大提高场景构建效率。提出基于分布式任务执行的高并发异步构建技术，确保了整套系统的高吞吐量，充分发挥服务器的性能，根据服务器性能动态调整任务执行进程的数量，避免服务器资源浪费或压力过大导致任务执行效率低下，实现了高效的并行计算。该技术已应用于大规模网络靶场构建之中，降低了复杂业务下的多重隔离和高并发异步靶场构建难度。	采用软件定义网络技术保障靶场场景与场景之间，任务与任务之间的数据隔离，保障实验数据的完整性和隔离性。基于多重隔离的消息队列，将外部消耗服务器资源的同步请求转化为异步请求，并按消息种类进行划分并发执行；实现任务调度、任务执行、后端存储和任务自动发现，大大提高场景构建效率。	网络靶场系列产品、安全、管控与蜜罐产品、网络安全竞赛服务
4	高性能动态可配置的容器服务承载集群技术	通过容器集群管理技术来承载Web服务，通过专有的描述语言文件定义、标准化的API接口来实现应用部署、更新迭代、横向扩容、可用性监控等一系列的运维能力。同时基于泛域名、内网DNS无配置文件解析自动寻址，基于去中心化虚拟节点方式，在不扩容集群硬件节点情况下，实现百万级容器服务承载。	通过专有的描述语言文件定义、标准化的API接口来实现应用部署、更新迭代、横向扩容、可用性监控等一系列的运维能力。同时基于泛域名、内网DNS无配置文件解析自动寻址，基于去中心化虚拟节点方式，在不扩容集群硬件节点情况下，实现百万级容器服务承载。	网络靶场系列产品、安全、管控与蜜罐产品、网络安全竞赛服务、安全工具类产品

(三) 高甜度诱捕的对抗式网络靶场核心技术

基于脆弱点感知的高甜度诱捕构建技术、内核级攻击行为全景捕获与复现技术、面向应激反制的交互式对抗环境生成技术、基于对抗的非接触高精度溯源反制框架技术和智能身份元数据萃取识别技术,大大提升了靶场的防御诱捕和对抗溯源能力。相关核心技术先进性的具体体现如下:

序号	核心技术名称	核心技术说明	核心技术先进性的具体体现	对应的产品或服务
1	基于脆弱点感知的高甜度蜜罐构建技术	针对传统的静态靶标系统伪装程度不高的现状,提出了脆弱点感知的靶机动态伪装技术,从靶标漏洞特征方面,靶标系统预置大量被攻击场景以及漏洞特征,同时具备了漏洞场景靶机实时的切换能力,满足攻击者不同意图、不同手段的“需要”。从靶标网站仿真方面,将模仿的目标网站样式、标题数据、栏目数据以及网站的外形进行高度模拟;从主机标识仿真方面将靶标主机名称等信息高度仿真;从网站内容仿真方面将靶标网站内容伪装成更像企业内部正在使用的网站;从网站通讯仿真方面,利用网站与数据库系统、其它网站网络层进行交互仿真,模拟真实网站的访问请求信息,包括数据库交互、网站间交互等。从而弥补了静态伪装、低交互式伪装程度不足、诱惑程度不够的问题,从而提升了网络靶场和蜜罐系统诱捕攻击者的能力。	利用网络渗透攻击者对系统的信息感知不对称性的原理出发,在场景相似度较高的情况下,根据部署的位置和特性出发设计出吸引攻击者关注和进行尝试的多种脆弱点,增加蜜罐系统作为陷阱吸引特定攻击者的能力,创新提出高甜度的概念,技术上能贴合攻击者秉性,增强对其的诱惑力。平台内置多种最新脆弱点并支持后台页面配置一键添加,可快速根据部署环境添加有吸引力的脆弱点增加网络靶场和蜜罐的诱捕效果。	网络靶场系列产品、安全管控与蜜罐产品、网络安全竞赛服务
2	内核级攻击行为全景捕获与复现技术	针对现实网络中被攻击的行为不能全量捕获,导致分析不够全面并且需要人工分析的问题,提出基于平行被攻击行为捕获和分析技术,对攻击者的攻击手段、攻击样本、攻击路径进行捕获,并从中分析出攻击者的攻击意图。在平行靶标中,采用基于内核级的行为监控方法,记录攻击者在靶标中的网络、文件、进程操作,并保存攻击者上传的恶意样本。在网络侧,采用旁路检测的方法,记录攻击者在网络上的攻击流量,并保存攻击载荷、样本信息。突破性的实现了通过关注局部、可全量记录的方式减少存储的消耗。全面加强了靶场内攻击行为数据全景捕获和分析能力。	通过对攻击行为的积累和研究总结为多条攻击行为和攻击模式模型,在内核的高权限空间中,对相应的行为系统状态变化进行监控,能隐蔽和全面的掌握多样性的攻击内容和精确的行为,避免攻击者利用优先启动或其他应用层手段绕过或发现监控,为网络靶场和蜜罐的数据采集等提供稳定高效的数据。	网络靶场系列产品、安全管控与蜜罐产品、网络安全竞赛服务、安全工具类产品
3	面向应激反制的交互式对抗环境生成技术	针对传统对抗环境下防御方处于被动状态无法发动有效的反击的问题,提出面向应激反制的交互式对抗环境生成技术,此技术是在威胁激励下通过感知和归因分析做出有目的的反制响应,采用浏览器指纹追踪、操作系统指纹追踪、攻击者社交ID追踪、诱饵数据追踪、标识植入方法,结合IP溯源技术,可以准确的发现攻击来源并可通过高伪装毒饵的方式开展反制,最终实现在对抗环境内对攻击者的行为的捕获、追踪、溯源和反击,从而提高了攻击诱捕、数据分析、反制的对抗环境模拟能力。	通过该技术的应用让产品可根据复杂环境中的交互印证(预制反制采集点)下,对攻击者采取灵活的反击手段,投放有针对性的蜜饵,在隐蔽的模式下通过攻击者对蜜罐的访问流量中的关键特征或隐秘数据进行解析和分析,最大化的获取攻击者相关信	网络靶场系列产品、安全管控与蜜罐产品、网络安全竞赛服务

序号	核心技术名称	核心技术说明	核心技术先进性的具体体现	对应的产品或服务
			息，实现更好的定位和溯源效果。	
4	基于对抗的非接触高精度溯源反制框架技术	基于攻击指纹 ID、攻击 IP、攻击手段、安全设备告警日志、服务器日志、应用日志、钓鱼邮件、恶意程序以及情报线索等，梳理出了针对不同攻击手段的溯源反制流程，可实现对指纹 ID 的分析与追踪、对攻击 IP 的分析与反渗透、钓鱼邮件的分析与反制、恶意程序的逆向分析与反连域名的追踪、对情报线索的深度利用，实现智能化的溯源反制框架。	对多种来源的各类数据进行模型化处理，利用大数据和模型匹配算法构建溯源反制框架技术，可基于统一接口下发策略和对接模块化的处置引擎，快速查找和匹配具有对应特征或参数的相关数据，对特定目标进行信息提取、关联分析和溯源等。	网络靶场系列产品、安全管控与蜜罐产品、网络安全竞赛服务、安全工具类产品
5	智能身份元数据萃取识别技术	采用基于协议结构和身份元数据进行特征萃取的方式，通过专有的算法训练得到身份元数据特征模板，形成身份元数据特征词词典，综合多种模式识别的方法，实现从数据中全面准确的提取身份元数据的目标。	基于网络标准协议、应用、行为等指纹技术进行身份识别，引擎和指纹库的分离，可以动态升级指纹库，利用多种指纹和特征的组合检索进行逐级筛选和定位，从海量异构数据中依据多种元身份萃取模型来提炼和定位目标身份，在身份模型复杂度级别、身份漏报率、结果准确率方面具有显著提升。	安全管控与蜜罐产品、安全工具类产品

（四）多维度的实战性网络攻防核心技术

恶意代码检测分析技术、漏洞挖掘及利用验证技术、基于单流特征与关联特征相融合的流量检测技术、模块化高并行即时计算平台技术、智能算法混淆加密视频处理技术和分布式存储及深度分析技术，分别从安全漏洞挖掘与利用、恶意代码检测、并行计算、数据防破解及大数据存储与分析等方面对产品给予支撑。

序号	核心技术名称	核心技术说明	核心技术先进性的具体体现	对应的产品或服务
1	恶意代码检测分析技术	该技术用于发现和定位已知和未知恶意代码。总结各种恶意代码对被感染系统的控制过程和留存方式，抓住恶意代码的核心行为特征，综合利用静态特征匹配与动态沙箱行为匹配相结合的方式，实现对恶意代码的发现和定位，尤其针对 APT 攻击过程中使用的特种隐藏型恶意软件，具有非常显著的效果。	通过将静态和动态两种恶意代码检测技术高效的结合起来，通过静态特征与动态行为模型相结合并引入专家判定模型的方式，自动化的对可疑样本进行分析和检测，发现常规恶意软件、变种或特种隐藏型恶意软件，具有速度快、	安全工具类产品、安全防护系列服务

序号	核心技术名称	核心技术说明	核心技术先进性的具体体现	对应的产品或服务
			效率高、误报率低等优点。	
2	漏洞挖掘及利用验证技术	该技术用于自动化的完成二进制代码漏洞挖掘和利用。利用靶场环境的多样性和资源快速调度的优势，结合智能 FUZZ 平台，根据既定策略快速生成多种变异的流量或文件样本，投放到被检测操作系统等信息系统中，同时利用靶场的全量数据采集和系统状态监控能力以及沙箱的精准行为监测能力，快速验证造成目标信息系统出现异常或故障的有效样本库，大大提升漏洞挖掘的速度和质量，同时验证环境还能漏洞利用代码的快速验证和留存积累提供良好的协作支持。	基于专家系统和漏洞模型，通过将模糊测试技术和虚拟化场景进行结合，快速构建智能化的漏洞样本及分析数据集，并利用数据采集分析技术发现样本可能造成的系统破坏和状态异常，最大化利用资源覆盖率和样本生成集合快速发现和验证漏洞的存在，并基于有模型生成利用软件，对结果予以验证，形成发现、利用、验证的高效自动化漏洞利用闭环模式。	安全工具类产品、安全防护系列服务
3	基于单流特征与关联特征相融合的流量检测技术	传统的流量检测方法只针对单包或者单流数据进行检测，但未通过把各流关联到一起进行检测。该技术提出基于单流特征与关联特征相融合的关联模型，该模型由单流内部流量特征的贝叶斯网络识别算法与多流之间行为特征的支持向量机识别算法组成，通过此关联模型，将确保准确性和效率，可大规模应用在实际环境中。	解决常规的基于单流特征匹配检测效率和准确性不足的问题，将关联特征和其他参数加入原有匹配规则内，利用新的模型提高准确率和检测效率。	安全工具类产品
4	模块化高并行即时计算平台技术	该技术是一套网络数据处理技术，专门针对多核 CPU 硬件平台进行设计，可充分发挥多核 CPU 的性能优势和效率优势，提供线程级高速并行计算能力，在接入层、分析层、控制层、响应层均提供相应的网络数据处理能力，用户可灵活通过管理接口对各层功能进行设置，提供良好的扩展性，支持插件开发的方式扩展功能。	基于 DPDK 简化裁剪而开发的专有技术，利用内核优化和多线程并发的异步技术，充分调动系统多种资源，大幅度的提高网络数据包的分析能力并具备良好的弹性扩展能力。	安全工具类产品
5	智能算法混淆加密视频处理技术	基于不可逆加密算法，采用多项行业先进技术对视频文件进行周密的动态保护、内置了自主研发的防注入、防调试及自变异特性等加密引擎和超高清数字解码引擎。支持动态的自适应流和平滑流，以及常用的视频格式；支持高级的流压缩特性；支持自定义和扩展使用场景；支持手机及平板等多种移动终端设备；支持视频水印，同时支持动态视频水印，保护版权；支持外置加密文件保持格式不变，同时支持自定义视频格式。	为了保护视频文件不被盗用，研发了专用的加解密算法，并在网页的视频播放器以及服务器端进行部署，对视频流媒体进行特殊的压缩和内存分块解密、水印叠加模式，具有加解密效率高，扩展性好的特点。	网络靶场系列产品、安全工具类产品
6	分布式存储及深度分析技术	基于大数据组建形成分布式基础数据存储分析架构，利用合理架构分布式数据仓库、海量数据收集、数据总线、计算框架、搜索引擎、交互式分析等组件实现对安全信息数据的接入与处理分析。联合使用实时流式分析、机器学习批式分析、交互分析等分析引擎，进行情报匹配检测、机器学习模型检测、关联分析、探索发现、事件追溯等分析工作。	通过先进技术的应用更加适合海量、多源、异构、分布场景下的情报数据的加载、融合、关联、检索等，形成数据、信息、知识的人机交互转化。	安全管控与蜜罐产品

三、结合核心技术在相关产品或服务中的具体应用情况，论证公司主营产品或服务均使用到相关核心技术的依据

（一）网络靶场系列产品

网络靶场系列产品主要包括赛事演练靶场、人才培养靶场、智慧城市安全测试靶场、案件线索追踪实战靶场、业务模拟仿真靶场、人工智能攻防靶场、复杂业务安全推演靶场及综合应用型网络靶场，作为网络空间的重要基础设施保障网络安全。网络靶场系列产品主要应用了网络空间平行仿真系列核心技术。

网络空间平行仿真技术中的“面向平行仿真的高性能靶场平台搭建与服务技术”是宏观性的，利用调度算法、QOS、智能多级高速 IO 缓冲区等技术总体解决了网络靶场高性能构建的问题。“基于混合虚拟化的属性平行仿真技术”“基于靶标分层同步的行为平行仿真技术”和“基于可扩展元场景的复杂业务模拟技术”，主要解决了网络靶场场景的高逼真度仿真问题，可以快速的将目标网络从架构、属性以及行为操作等各个层面实现模拟和仿真，并将其复杂业务间的依赖关系、时序关系等同步采集和复现到网络靶场中。“基于镜像差分压缩和分级存储的节点快速重构技术”和“基于多重隔离的高并发异步靶场构建技术”，解决了网络靶场在实际运用过程遇到的高并发性、高稳定性、可扩展性情况下的实现问题，可确保靶场同时并发承接多个复杂的业务场景构建，并保证任务与任务之间的数据隔离和网络隔离，确保实验数据的清洁和性能一贯性。

综合应用型网络靶场典型应用是 2020 年建成的网络安全科技馆，该馆是公司赛事演练靶场、人才培养靶场、业务模拟仿真靶场和智慧城市安全测试靶场的多场景综合性应用，运用了公司“基于混合虚拟化的属性平行仿真技术”“基于靶标分层同步的行为平行仿真技术”“基于可扩展元场景的复杂业务模拟技术”等多个网络靶场相关的核心技术。

（二）安全管控与蜜罐产品

1、春秋云阵新一代蜜罐系统

蜜罐综合应用了网络空间平行仿真技术和网络空间攻防对抗技术。

平行仿真技术中的“基于混合虚拟化的属性平行仿真技术”“基于靶标分层同步的行为平行仿真技术”和“基于可扩展元场景的复杂业务模拟技术”使得春秋云阵蜜罐可以快速的模拟和仿真被防护网络的特征，增加蜜罐场景的隐蔽性和

仿真度，使得恶意攻击者难以发现蜜罐的存在。

网络空间平行仿真技术方面的“基于脆弱点感知的高甜度蜜罐构建技术”解决了蜜罐产品的场景高甜度的场景构建问题，在被防御网络内部署更加能够吸引到攻击者的最新的安全脆弱点，让攻击者以为有机可乘，提出了基于攻击者视角的脆弱点感知的核心构建思想以及实现方式，从而诱捕攻击者触碰和进入蜜罐，进而被发现。

“内核级攻击行为全景捕获与复现技术”从攻击者行为捕获的角度出发，提供更准确的深层、隐蔽高权限行为监测分析，提供全方位、全景的视角，提升产品的应用价值。

“面向应激反制的交互式对抗环境生成技术”和“基于对抗的非接触高精度溯源反制框架技术”分别从典型应用场景出发，提供了从反制对抗生成到技术框架的解决方案。

2、春秋云势网络安全态势感知与处置平台

春秋云势网络安全态势感知与处置平台主要运用了“分布式存储及深度分析技术”“智能身份元数据萃取识别技术”，解决以往安全防御体系中“重数据统计、轻威胁处置”的问题。网络靶场相关技术的创新性引入，使平台产品实现了快速定位网络安全威胁并进行高效处置的能力，切实提升网络安全有效性。平台将海量的各类报警数据、处置过程和结果数据等进行快速的分布式存储，利用分布式的数据仓库、高速数据总线、分布式搜索引擎、交互式分析等组件实现对多种厂商、多种类型设备报警数据的存储、清洗和处理，依托于平台提供的易用人机交互界面可以快速的构建数据分析模型，从海量的数据中自动匹配和发现网络中的异常情况，利用其中的终端指纹、行为特征等定位嫌疑人等。同时评估网络系统当前的各类安全指数，预测未来一定时间内的安全态势变化等，并依托于流程化、高精细度的处置过程管控来实现对处置资源的合理调配和跟踪。

3、安全管控

结合春秋云阵蜜罐和春秋云势网络安全态势感知与处置平台的技术优势，将公司网络靶场技术中的平行仿真系列技术与“分布式存储及深度分析技术”“智能身份元数据萃取识别技术”结合运用，实现蜜罐“零误报”的特性与安全管控的“高处置”特性相结合，实现快速的发现和捕获 APT 攻击，留存攻击行为日志

和各类黑客攻击工具样本，快速识别可能的黑客组织线索，协助安全防御用户追踪溯源，定位黑客攻击者的能力，大大提升网络安全防御的有效性。

（三）安全工具类产品

1、流量监测类产品

主要利用“基于单流特征与关联特征相融合的流量检测技术”，将传统的单一流量特征与关联流量特征相融合，利用相关特征模型识别和发现网络流量中的异常流量，并辅助以公司在针对加密异常流量的分析算法和模型，快速的从海量的网络流量中捕获可疑或异常流量并自动化进行流量内的内容匹配和分析。

2、数据分析类产品

主要利用“恶意代码检测分析技术”和“内核级攻击行为全景捕获与复现技术”相结合，构建自动化快速恶意代码行为记录及分析工具、海量智能样本生成及验证工具等，批量的处理导入的流量或文件样本，发现其中的恶意代码、可疑文件等，输出该代码执行后对系统的各种修改记录和行为。

3、业务支撑类产品

基于“漏洞挖掘及利用验证技术”“模块化高并行即时计算平台技术”等开发的多种工具，用于网络安全的各种业务目标突破、密码匹配、模型推演、自动化挖掘等方向。

4、安全辅助类产品

单独或混合利用“高性能动态可配置的容器服务器承载集群技术”“智能算法混淆加密视频处理技术”“基于对抗的非接触高精度溯源反制框架技术”“智能身份元数据萃取识别技术”等研发的各类辅助类工具，涵盖进行特定模型匹配的高性能计算基础平台、保护相关数据防破解软件、人员及组织身份关联检索及分析系统、针对特定任务的溯源反制工具等。

（四）安全防护系列服务

依托公司的多种网络攻防核心技术以及自主研发的工具集合，采用标准化的服务模式和靶场等平台，将安全服务人员的能力提升、服务过程中的全生命周期数字化管控与安全能力相结合，为客户提供各类高级别的安全服务。在进行安全防护的过程中，会利用到公司自研的多种网络安全工具、蜜罐系统、网络靶场系统平台等完成数据采集、网络安全防御和对抗、数据取证、大数据分析、黑客攻

击溯源反制、日志备份与检查、应急响应、安全加固等各类安全服务工作。

（五）网络安全竞赛服务

无论线上还是线下的各类竞赛服务，均重点依托公司成熟的网络靶场平台相关核心技术，可快速进行赛事的部署和实施，应对多种赛制、竞赛模式、积分方式及赛题类型等，结合公司的运营服务优势，在竞赛服务的规模、稳定性、工程化能力以及成本控制方面具有优势。

（六）其他服务

1、线上安全培训

发行人所使用的课程体系和培训教材多为标准化的产品，内容标准化且课程时长固定。注重技能培训过程中的实践动手能力的提升，以及网络安全方法论的实践，学员在观看课程视频的基础上，注重提供以助教指导线上实操训练，线上实操训练基于公司的网络靶场平台，使用了公司的核心技术。

2、线下安全培训

发行人线下安全培训中依托于网络靶场平台，包含硬件系统、教学管理系统、视频播放系统、能力考核系统、实操训练系统、仿真场景系统、资源管理系统、课件资源包等软硬件，同时配有木马查杀、安全漏洞等标准化的课程内容。线下安全培训基于公司的网络靶场平台，使用了公司的核心技术。

四、公司核心技术收入占比

公司线上培训以及线下培训存在课程以及讲师通过外购或外聘，基于谨慎性考虑，在核心技术产生的收入中剔除；网络安全科技馆综合利用了公司主要产品以及其他网络安全产品，虽然将网络安全科技馆总体作为公司网络靶场的综合应用，使用了公司的核心技术，外部采购项目作为网络安全科技馆的成本，但鉴于非公司网络靶场相关的展项外部采购金额较大，基于谨慎性考虑，在核心技术产生的收入中剔除网络安全科技馆中非公司网络靶场相关的展项产生的收入。具体如下：

收入分类	是否列为核心技术收入	备注
网络靶场系列产品	是	2020 年核心技术收入剔除了 2020 年“网络安全科技馆项目”中非公司网络靶场相关的展项产生的收入
安全管控与蜜罐产品	是	全部列为核心技术收入

网络安全工具	是	全部列为核心技术收入
安全防护系列服务	是	全部列为核心技术收入
网络安全竞赛服务	是	全部列为核心技术收入
其他服务	否	-

公司主要以“项目制”开展业务，公司产品主要以软件或软硬一体化形式体现，软硬一体化形式主要是公司采购相应的服务器等 IT 硬件产品，进行组装调试，然后将软件灌装入硬件设备中，外部采购的硬件作为整个项目的成本，是整个项目的组成部分，公司并不从事产品化软件、硬件的销售贸易业务，核心技术产生收入无需剔除外购软硬件产生的收入。

公司核心技术产生的收入及其占比如下：

单位：万元

项目	2021 年 1-6 月	2020 年	2019 年	2018 年
核心技术产生的收入	7,812.74	22,872.28	15,246.66	17,077.44
营业收入	8,136.08	29,164.20	16,308.54	18,051.03
占比	96.03%	78.43%	93.49%	94.61%

(4) 结合在手订单及业绩预计情况等，说明发行人是否持续符合科创属性评价指标。

【回复】

一、在手订单情况

截至 2021 年 11 月 30 日，公司正在履行的合同金额为 22,854.61 万元，合同数量为 115 个，具体情况如下：

单位：万元

合同金额区间	2021 年 11 月 30 日	
	合同数量	合同金额
大于 1,000 万	5	7,543.24
500 万-1,000 万	10	6,729.52
100 万-500 万	28	6,327.57
50 万-100 万	16	1,218.48
10 万-50 万	33	939.57
小于 10 万	23	96.22
合计	115	22,854.61

二、业绩预计情况

公司 2021 年的业绩预计情况如下所示：

单位：万元

分类	金额
截至 2021 年 11 月 30 日已确认收入（不含税）	20,226.48
截至 2021 年 11 月 30 日在手订单（含税）	22,854.61
12 月预计签单项目（含税）	13,912.23

截至 2021 年 11 月底，发行人在手订单金额达到 22,854.61 万元，其中 16,099.36 万元未确认收入，在手订单较为充裕，业务拓展情况良好，业务开展的可持续性较好。预计公司 2021 年全年收入超过 30,000.00 万元。

综合来看，网络靶场业务仍处于起步阶段，根据客户需求，可叠加不同的功能模块和应用系统，单个项目收入的增长潜力较大。尽管网络安全科技馆建设项目具有偶发性，公司的在手订单充裕，业务扩展情况良好，公司业绩具有可持续性，发行人持续符合上市标准。

三、科创属性评价标准

1、最近 3 年累计研发投入占最近 3 年累计营业收入比例 $\geq 5\%$ ，或最近 3 年累计研发投入金额 $\geq 6,000$ 万元

公司 2018 年-2020 年研发投入分别为 4,347.00 万元、3,544.59 万元、3,847.85 万元，合计 11,739.43 万元，占最近三年累计营业收入的比例为 18.48%。公司重视研发投入，随着未来公司的不断发展及规模不断扩大，研发投入预计将不断增加，持续满足研发标准。

2、研发人员占当年员工总数的比例 $\geq 10\%$

2018 年-2020 年末公司研发人员占比分别为 53.75%、44.01%、43.44%，2020 年末为 43.44%，超过 10%。公司所处网络安全行业为技术密集型行业，研发人员占比较高，不断提高公司的核心技术水平，公司将持续满足研发人员比例标准。

3、形成主营业务收入的发明专利（含国防专利） ≥ 5 项

公司及其子公司已取得 9 项授权发明专利，在审专利若干，公司专利均形成了主营业务收入，公司持续符合发明专利标准。

4、最近三年营业收入复合增长率 $\geq 20\%$ ，或最近一年营业收入金额 ≥ 3 亿

公司 2018 年-2020 年实现营业收入分别为 18,051.03 万元、16,308.54 万元和 29,164.20 万元，复合增长率为 27.11%。公司预计 2021 年营业收入超过

30,000.00 万元，随着公司的不断发展，公司未来规模将持续在年营业收入 30,000.00 万元以上，公司将持续符合营业收入标准。

【核查程序】

保荐机构及发行人律师执行了以下核查程序：

- 1、获取网络安全行业相关法律法规、行业政策，访谈发行人主要负责人，核查公司主要业务是否符合国家科技创新战略要求；
- 2、获取发行人产品销售许可证，核查相关证书是否处于有效期内；查阅相关法律法规及同行业可比上市公司案例，核查发行人产品除蜜罐产品和安全工具类产品外，是否需要具备相关资质，核查发行人产品特征和部分产品未列入相关名录的情况是否符合行业惯例；
- 3、获取发行人发明专利证书，访谈发行人主要负责人，了解发明专利在核心技术中的具体应用；访谈发行人核心技术人员，了解发行人核心技术在主要产品中的具体体现；
- 4、获取网络安全行业研究报告，访谈发行人主要负责人，核查公司主要产品及服务是否属于网络安全行业以及划分领域；
- 5、查阅网络靶场相关行业研究报告、行业相关新闻报道，了解公司网络靶场等主要产品的行业地位；
- 6、访谈公司主要客户以及终端客户、访谈公司人才培养学员，了解其对公司主要产品的看法，验证公司行业地位的情况；
- 7、获取公司在手订单明细并访谈公司总经理、财务总监，了解公司业绩预计情况；
- 8、获取公司及主要产品获取的奖项，验证公司行业地位的情况；
- 9、获取发行人审计报告、员工花名册及发明专利证书等，核查公司是否符合科创属性评价标准。

【核查意见】

经核查，保荐机构及发行人律师认为：

- 1、发行人产品属于网络安全产品，业务实质为软件而非系统集成；
- 2、发行人主营业务和主要产品符合科创板支持方向、科技创新行业领域和相关指标等科创属性要求。

2、关于主营业务

2.1、关于网络靶场业务

根据申报材料：（1）公司业务类型包括网络安全产品和网络安全服务两大类，其中网络安全产品分为网络安全靶场与人才培养、安全管控与蜜罐和安全工具类产品三个子类；（2）发行人以项目制组织方式开展业务，各项目可以为标准化产品、定制化软件产品、硬件、服务的组合形式；（3）网络靶场是公司的核心，是网络安全人才培养不可或缺的产品体系，是用户网络安全保障重要的基础设施，发行人研发了具有自主知识产权的网络靶场平台-春秋云境网络靶场；（4）2018 年公司推出国内首个城市级网络靶场，确立了公司在网络靶场领域的行业领先地位。

请发行人披露：

（1）结合具体业务场景，用浅白语言披露公司网络靶场业务的实质、实施方式，所提供产品或服务的具体内容，与同行业网络靶场业务的区别；（2）区分软件、硬件和服务，分别披露报告期各年度的销售金额及占比情况；（3）剔除网络安全科技馆建设项目影响，公司网络安全产品毛利率逐年下降的原因。

请发行人说明：（1）将网络靶场、人才培养业务列为网络安全产品而非网络安全服务的依据，报告期各期网络靶场业务、人才培养业务（区分线上和线下）的项目数量、收入及占比、毛利率、前五大客户情况；（2）公司春秋云境网络靶场平台与公司网络靶场业务的关系，是否主要用于支撑网络安全演练活动和人才培养，该平台是如何作为基础设施保障用户网络安全的；（3）网络靶场业务领域的竞争格局、发展趋势，公司在网络靶场领域处于“行业领先地位”的表述依据是否充分。

请保荐机构对上述事项进行核查，并发表明确意见。

【回复】

请发行人披露：

（1）结合具体业务场景，用浅白语言披露公司网络靶场业务的实质、实施方式，所提供产品或服务的具体内容，与同行业网络靶场业务的区别；

一、网络靶场业务实质

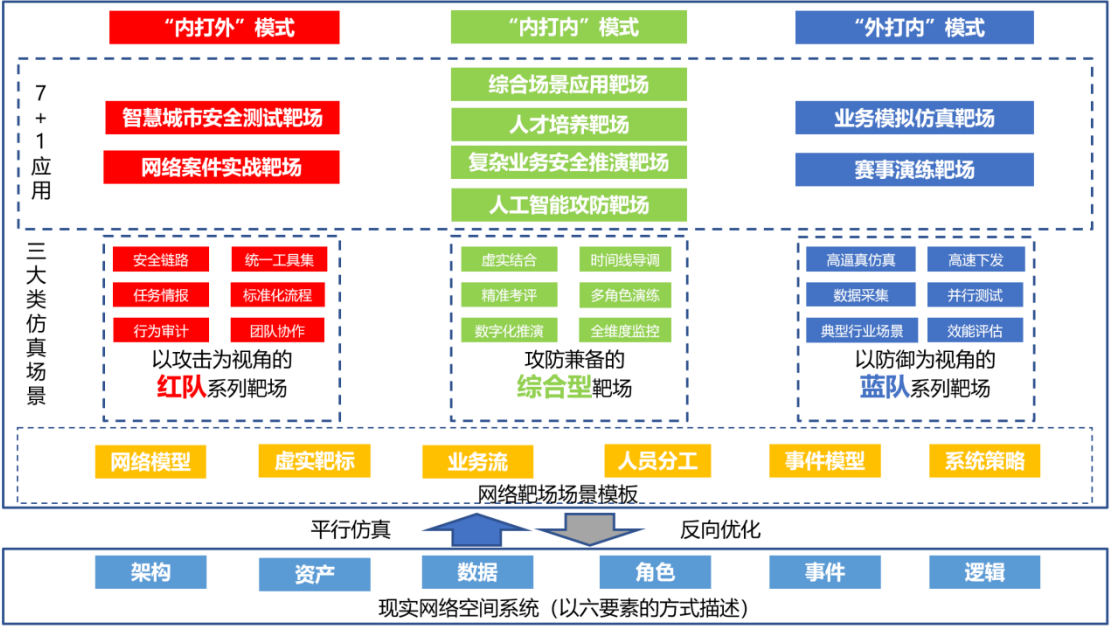
网络靶场存在多种应用模式，既可以在靶场中模拟仿真各类高逼真的大规模

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。

根据网络靶场专家方滨兴院士及鹏城实验室网络靶场介绍，网络靶场是一类网络系统的仿真平台，服务于网络安全人才培养、网络攻防演练、网络安全产品评测和网络新技术验证等，用于提升和加强网络系统的安全性、稳定性和性能。主要分为三种不同攻防形态，内打内、内打外、外打内。

内打内指攻击手和被攻击目标均在靶场内，在完全可控的环境中完成相关业务活动，典型应用场景为攻防对抗实训场景、安全方案或产品的内部测试测评等；内打外指从靶场内部向外部真实目标发起测试，测试人员基于靶场提供的统一环境来完成任务，重点是快速的为成规模的测试人员提供统一可靠并且条件完备的任务操作环境和链路等支持，并且实时的全面记录和管控测试行为并做审计，典型应用场景为科研或监管单位或部门对实网进行的各类安全测试和评估等；外打内主要指利用靶场平台的快速场景构建能力和场景克隆复制能力，将被验证或测试的目标系统或目标网络生成于网络靶场内部，并根据相应的访问策略对互联网开放，所有具备授权的测试者均可以通过互联网对这个场景进行测试，而在测试过程中，靶场详实的记录测试者在靶场内的各种行为和对被测场景造成的影响，并进行各类评估和展示等，典型应用场景主要用于大规模产品测试、众测、多靶场场景间的联合测试、在线攻防竞赛、蜜罐蜜网防御等。

平行仿真技术是春秋云境网络靶场的核心。平行仿真是基于自主研发的专有云平台，以虚拟化为主、虚实结合为必要手段，通过模拟仿真与现实网络空间相对应的场景模型，并在其中进行一系列的安全功能应用，让仿真环境中所产生的结果平行影响真实业务系统的网络安全防御的技术体系。平行仿真技术为网络空间积极防御构建了攻防兼备的综合性网络靶场、防御视角的蓝队系列网络靶场以及攻击视角的红队系列网络靶场，支撑了网络空间的测试、演练、实训、推演、研判、指挥、防御、实战等综合性网络安全业务。



平行仿真技术主要应用在三类网络安全场景：第一类是攻防兼备的综合型网络靶场，能够还原完整的网络安全攻防对抗事件以及配套的网络环境，包含使用到的资产和装备、各方角色模拟等，通过完整复刻真实发生的重大安全事件，让使用者参与事件细节，提升实战水平，以强化网络安全防御能力；第二类是防御视角的蓝队系列网络靶场，主要仿真的是防御或测评类目标的相关场景要素，目的是在不对实网环境造成破坏影响的前提下，尽可能检验和发现真实环境中存在的问题和风险；第三种是攻击视角的红队系列网络靶场，主要仿真的是各种常见的典型攻击场景或者针对某种特定目标设置的专项场景，涵盖网络环境、资产（装备）、相关的已知情报数据、权限分工、状态变化等。通过将红队的网络阵地、资产装备、身份隐藏、行为伪装等要素融合成一个可控的、高效的标准化场景，进行集约化、专业化、安全化的管理。通过攻击者的角度将红队的工作环境和战法固化成标准状态，以提升测试效果并保障自身的安全。

网络靶场业务的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。此外，公司还利用网络靶场核心技术研发了安全管控与蜜罐产品，作为欺骗式防御产品，有效帮助客户提升安全防御能力。

二、不同场景的实施方式以及所提供产品或服务的具体内容

（一）网络靶场系列产品

公司网络靶场系列产品主要包括以下类别：

序号	靶场类别
1	赛事演练靶场
2	人才培养靶场
3	智慧城市安全测试靶场
4	案件线索追踪实战靶场
5	业务模拟仿真靶场
6	人工智能攻防靶场
7	复杂业务安全推演靶场
8	综合应用型网络靶场

上述产品的具体内容以及在不同场景中的实施方式和内容具体如下：

1、赛事演练靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，人才培养是未来的一大发展目标，要求建成一批网络安全人才实训基地、公共服务平台和实训靶场，创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人才规模质量不断提高。赛事演练靶场正是这一目标下的典型应用场景。

“网络安全的本质在对抗，对抗的本质在攻防两端能力较量。”网络安全赛事可通过网络对抗的模式检验参赛队伍的实战攻防能力和应急协作水平，整个过程需要在专门搭建的、符合行业特征的、安全可控的演练环境中进行，通过竞技形式有效训练选拔网络安全人员。

赛事演练靶场主要采取外打内模式。赛事演练靶场平台提供完备的赛前、赛中、赛后管理功能，支持多种可选的比赛模式、积分计算模式以及配套的多种大屏展示效果。赛事组织方可利用靶场平台自定义赛题或从已有题库和场景库中选择赛题一键下发竞赛，靶场依据策略自动化完成资源管理、数据记录和分析等各类操作。

参赛选手利用分发的账号密码权限登录到靶场平台，获取平台预设好的竞赛靶标进行解题，根据竞赛或演习目的不同，靶标可分为寻找线索类、对抗类、分析类、仿真场景类等多种。同时，平台裁判员也会通过靶场平台对赛事过程进行

管理，包括暂停和恢复竞赛、根据平台报警处置违规行为、发布公告及加减分工作等。在举办网络安全赛事时，赛事演练靶场会以软硬件一体的方式部署在赛场或线上，靶场设备独立组网与每一个参赛选手终端联通。

公司赛事演练靶场业务的典型应用，以“巅峰极客”网络安全技能挑战赛为例。根据合同约定，公司负责 2018 “巅峰极客”网络安全技能挑战赛中线下决赛的关键信息基础设施靶场平台定制服务，具体包括：在平台中提供系统管理模块，供平台系统管理、参数设置、界面管理、人员管理等功能使用；在平台中提供竞赛管理模块，提供全面的竞赛过程管理功能，管理员可对竞赛过程中的竞赛行为进行监控和管理；在平台中提供题目管理模块，管理员可以根据竞赛要求，对竞赛题目模式、类型、数量等进行选择，并对相应题目进行分值设定；在平台中提供竞赛展示模块，主要包括竞赛人员答题界面和竞赛过程展示界面，竞赛裁判或者观众可以通过此界面实时了解各参赛人员的得分情况。

该赛事是中央网信办指导的 2018 年国家网络安全宣传周官方赛事，大赛高度模拟仿真了能源、电力、金融、交通、电信等十余个关键信息基础设施仿真场景，支持 8 种角色在其中进行“真攻真防”技能演练。由渗透测试团队针对虚拟的城市网络体系展开渗透测试；由关键基础设施防御、基础设施业务人员和普通网民、供应链业务系统、网安监管、IT 系统、竞赛裁判及靶场系统运维等 7 个团队组成联合防御队，对抗渗透测试团队对网络的破坏，构筑关键信息基础设施网络系统安全防线。通过赛事演练靶场，一方面检验不同参与角色实战能力；另一方面验证关键信息基础设施和重要信息系统在实战演习演练中的安全防御水平和应急响应能力。



2、人才培养靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，人才培养是未来的一大发展目标，要求建成一批网络安全人才实训基地、公共服务平台和实训靶场，创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人才规模质量不断提高。人才培养靶场正是这一目标下的典型应用场景。

网络安全人才培养需要体系化的课程安排及大量的训练和实践，还需要进行高强度的学习考核计划安排。人才培养靶场就是为人才实践训练和体系化的培养训练专门打造的培训平台。在人才培养靶场平台中，教师和学生分别用自己独立账号登录到靶场，教师在靶场进行教学和考核任务下发，将靶场中自带的课程、实验、题目的学习或考核任务下发给学员，并观察学员培训和考核进展；学员登录到靶场，进行学习和实验训练，也在靶场中进行技能考核。

人才培养靶场是网络靶场的典型应用之一。网络安全攻防对抗具有其特殊性，技能能力的提升必须依赖反复的动手实践才能完成。而网络安全的各类漏洞和攻防技战法对技能要求的多样性非常高，而网络靶场利用虚拟化和云技术，使各种典型或特定的场景以虚拟机和场景快照模板的方式留存下来，因而可以快速的为人才培养提供各种演练的场景和环境。

在院校或者企业进行人才培养时，人才培养靶场通常以软硬件一体化的方式部署在学校或企业的内网环境，靶场会配置内网 IP 地址，管理员建立和分配教师、学生的账号。教师和学生分别用独立账号登录到靶场。

公司人才培养靶场业务的典型应用，以北京航空航天大学靶场项目为例。根据合同约定，公司提供 e 春秋网络安全实训系统，通过组建专业的网络安全实验室，主要承担信息安全本科专业的教学实验，内容涵盖信息安全专业的主要课程，通过专业设计、创新应用的实验仿真环境，帮助学生可以快速构建实验场景，有效提升学生实践动手的能力。



3、智慧城市安全测试靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，打造网络安全“靶场云”，建设数字孪生靶场，为城市安全能力验证等提供支撑。智慧城市安全测试靶场正是这一目标下的典型应用场景。

在数字化城市的建设过程中，实际上存在大量的数字建设的网络安全风险，在用传统手段发现隐患的同时，还可以通过网络安全测试发现更多风险隐患。在进行安全测试时，测试人员的操作违规或误操作均可能会给系统带来严重的风险隐患，从而导致城市的正常业务运转出现风险。因此业界急需能够对测试人员的测试流程、测试手段等进行标准化和精细化管控，也需要能够在测试中及时辨认和终止这些危险操作并进行自动化的控制，智慧城市安全测试靶场解决了这个难题。

智慧城市安全测试靶场可根据测试组织方的需要为测试团队和人员提供统一的以虚拟机场景为载体的测试操作环境，并使用经过验证和授权的统一链路进行网络安全测试。靶场提供了丰富的操作场景模板库，在每个操作场景中，根据测试任务的需要配置不同的操作系统、经过安全检查和验证的检测工具，防止任何因为测试人员自身的疏忽而将危险的病毒或木马等代入测试目标的情况。操作场景中利用靶场的数据采集技术，对操作行为从操作系统内核、应用以及数据流量等多个层面进行全面行为监控、恶意流量监控，并实时进行屏幕录像留存，一旦发现危险行为，平台会自动切断网络连接并进行后台报警提示，避免危险的发

生。同时，平台将网络安全的服务过程节点化和电子流程化，使每一个安全测试人员的操作均遵循标准的网络安全测试流程和步骤进行，保障安全测试过程和结果的可控可查。

参与测试的人员需要在可控的环境中进行操作，利用与其个人身份绑定的账号权限登录到靶场平台为其独立分配的测试靶场机中，每个账号所使用的测试环境资源均严格隔离，通过靶场机上分配的互联网或内网地址，访问测试目标，检测网络安全风险，测试过程必须在靶场机中完成，靶场会监测测试人员的操作行为，尤其是高风险行为会进行实时的自动报警提示，并赋予管理员阻止非法操作的权限，可设定为自动阻断或人为确定后阻断等。

智慧城市安全测试靶场一般以软硬件一体化的方式部署在互联网或政府指定的内网中。参与测试的安全人员，通过指定的测试账号，接入到靶场中，领取测试任务，并在独立分配的测试靶场机中进行任务操作。

公司智慧城市安全测试靶场业务的典型应用，以广东省数字政府“粤盾”系列测试为例。根据合同约定，公司提供广东省“数字政府”网络安全深度测试服务，为甲方召集并审核技术人才，不定期地对客户指定地“数字政府”政务应用系统开展深度渗透测试，模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，找出未知系统中的脆弱点和未知脆弱点，从攻击者的角度评估，向客户提交发现的安全隐患。通过在安全可控的靶场平台中，对相关系统和网站开展“数字政府”网络安全深度测试工作，常态化检验数字政府信息系统安全性。通过累计针对 21 个地市和省直机关数千个重要信息系统开展攻防测试，发现并消除了大量安全隐患。



4、案件线索追踪实战靶场

重点行业在进行案件侦办过程中存在两个比较突出的问题，一是任务人员的工具类型和使用不规范影响任务完成效率，这种状况也使人员的规模化培养以及形成团队战斗力遇到了障碍。二是任务人员自我保护意识和能力不足，容易被目标对象发现从而影响任务效果。

为解决上述问题，使案件线索追踪实战制式化、装备化，并提升自我防护难题，结合客户业务特性和需求研发了案件线索追踪实战靶场。首先，网络靶场统一管理所有对外链路并形成链路池，可以动态的根据任务要求进行链路的选择或动态切换，统一的链路管理杜绝了被目标发现和反制的风险。其次，统一人员操作环境，凭借网络靶场虚拟机快照和场景库，为各种任务目标和要求准备多样化的标准或定制操作环境，在环境中根据任务要求提供专业规范的工具库，并赋予每个人员独立安全的空间，任务信息及相关关联数据等均根据任务要求实时下发。由于每个人员的操作环境的独立性，任务相关的结果数据和过程数据等均严格隔离，数据的流入和流出均遵循相关安全要求并审计记录，可保障数据安全性。第三，操作环境和操作工具的统一化和制式化，为人才的培训和团队建设等均提供了基础，详实记录的过程数据也使基于靶场平台具备了复盘讲解和总结推演能力，大大提升了团队效率和业务能力。

在进行案件侦办过程中，靶场通过软硬件一体化的方式同时部署在互联网和客户内网。任务管理者可以指定任务的完成人或完成团队，并将任务进行拆解下发，可设定每个任务完成人使用的操作环境及环境中的配套资源和链路，实时查看任务的进度情况进行任务调配等。任务完成人员则利用身份信息和权限登录靶场平台，利用靶场中专门克隆出来的指定操作环境执行相关任务，任务结束后靶场清理和回收资源。

公司案件线索追踪实战靶场业务的典型应用，以公安部门案件线索追踪项目为例。根据合同约定，公司提供复杂网络虚拟化复现及安全演练系统，配置基础网络场景模拟推演靶场装备、一体化作战系统等软硬件产品，仿真网络环境构建、模拟设备，集成主流专用仿真链路场景。可用于攻防任务结束后的案件重演，利用拓扑图结合动画展示渗透路径、防御状态等，对仿真场景中的安全事件进行展示。靶场平台已支撑全国多个省市公安机关开展相关案件追踪活动，开展实战案

件侦办。支持公安部及各省、自治区、直辖市公安机关开展了多次的案件实战任务。



5、业务模拟仿真靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，积极推进网络靶场技术研究，建设结合虚拟环境和真实设备的安全孪生试验床，提升网络安全技术产品测试验证能力。国家能源局《关于加强电力行业网络安全工作的指导意见》中提到，建设网络安全仿真验证环境，适应电力行业网络安全研究、测试、演练等应用需求，整合现有资源，建立覆盖发、输、变、配、用、调度全环节的网络安全仿真验证环境。业务模拟仿真靶场正是这一目标下的典型应用场景。

工业环境对生产系统连续性要求极高，当遭遇网络安全风险时几乎不可能停机进行检修，开展安全测试、技术验证、病毒样本采集分析、模拟风险预警演练等工作，均需要在模拟仿真环境中进行。业务模拟仿真靶场提供了完善的仿真场景构建能力，基于公司多年来积累和沉淀的靶标库和基础场景库、行业仿真场景库等，具备了快速进行行业业务模拟的能力；业务模拟仿真靶场利用模拟仿真的靶场场景提供测试测评、攻防演练、效能评估、科研研发等多种功能。

各个行业的业务存在较大差异，不同的企业或单位的业务网络及应用系统即存在共性也存在各自的特点和特性，而其安全性也相应的具备共性或特性的脆弱点。进行业务模拟仿真，需要利用网络安全的视角了解和分析相关网络的各类要素，并进行提炼和浓缩，将网络安全与业务领域进行融合从而完成仿真和模拟。网络靶场将这些融合的结果沉淀为场景库中的多个场景模板和大量的单机靶标

模板。用户可以利用后台功能快速的基于这些基础元素进行调整和定制生成自己企业或单位的仿真场景，并以这些场景来进行各类实训、演练或测试测评活动。

管理者利用账号登录靶场后可进行场景构建、用户管理、任务管理、数据分析、复盘推演或演练测评等各类工作。操作用户则可以在登录靶场后查看被分配的任务、申请场景资源，在场景中完成各种任务并提交数据。靶场支持多任务并发，任务与任务之间数据和资源完全隔离互不干扰，同一任务的不同人员之间可根据任务管理的设定隔离或共享相关资源和环境。不同角色的人员接到各自任务后，在靶场仿真的环境中执行对应的网络安全测试或验证任务。同时，在靶场平台会记录、分析和展示任务的数据、过程和结果。

业务模拟仿真靶场依据用户需要，一般以软件或软硬件一体化方式部署在用户内部网络中。为了达到特定的仿真逼真度，通常会与用户的实体仿真工业设备进行联通。

公司业务模拟仿真靶场的典型应用，以某电网公司网络靶场建设为例。根据合同约定，公司提供网络安全靶场平台及相关能力建设，可实现搭建的虚拟网络拓扑与实体网络环境进行对接，并构建定制化场景，实现对接实体设备并共同组网。针对电力行业搭建病毒查杀验证靶场环境，选取部分病毒样本，并将病毒样本分别植入行波测距分析系统、数字式电力故障录波装置、故障录波管理机等设备进行查杀测试，持续开展工业仿真场景安全测试验证。



6、人工智能攻防靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，研究人工智能系统可解释性、隐私性等安全要素，突破人工智能模型攻击与防御关键技术，设计实现人工智能系统自动攻防平台，构建人工智能安全靶场。人工智能攻防靶场正是这一目标下的典型应用场景。

人工智能攻防研究是网络安全领域比较前沿的研究方向，需要对人工智能网络攻防对抗有效性和安全性进行研究验证。由于是程序进行自动攻防验证，对于测试目标的资源消耗较大，且会极大影响目标网络性能，甚至会对测试目标的网

络造成破坏，需要在安全可控的环境中完成自动测试。靶场提供了安全可靠和灵活的测试环境，还可以自动记录测试参数判断是否达到研制预期效果。用户开发完成人工智能攻防程序后，将程序上传到已经设定好测试环境和靶标的靶场环境中，接到下发的任务指令后，人工智能程序会自动开启攻防测试，靶场中的代理程序也会实时监控环境的稳定性并记录人工智能程序的测试结果是否达到预期目标。人工智能攻防靶场通常以软硬件一体或软件形式部署在独立的网络中，不与用户的办公或生产网络相连。

公司人工智能攻防靶场业务的典型应用，以某自动化测试靶场项目为例。根据合同约定，公司研发一套网络安全领域先进、智能、专业、完善的智能网络攻防比赛系统，即人工智能实验场。依托公司人工智能网络安全靶场平台，将客户自研的人工智能攻防机器人投放在靶场中，对靶场中的靶标进行自动化攻防，通过靶场高柔性的网络环境，在人工智能攻防机器人极具破坏性的测试过程中，确保测试环境的有效性和一致性，并在靶场中实时记录测试数据，统一对人工智能攻防机器人进行效能评估。



7、复杂业务安全推演靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，积极推进网络靶场技术研究，建设结合虚拟环境和真实设备的安全孪生试验床，提升网络安全技术产品测试验证能力。国家能源局《关于印发 2021 年电力安全监管重点任务的通知》中要求，推进电力行业网络安全仿真验证环境（靶场）建设，组织开展电力行业网络安全攻防实战演练。复杂业务安全推演靶场正是这一目标下的典型应用场景。

在真实的网络空间中，影响国家安全的网络安全问题通常由多种行为或风险叠加形成，为了预判和风险化解，需要在复杂的大规模推演靶场中利用数字模型

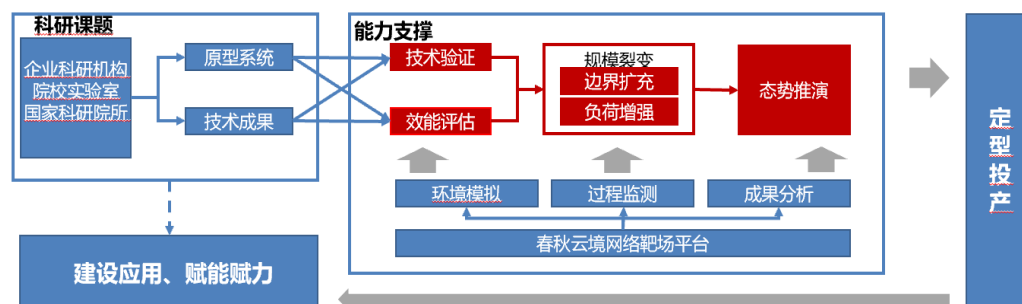
和模拟仿真技术等进行仿真推演。进行推演时，靶场管理员登录靶场，在靶场中利用靶场机和专业物理设备（如物联网设备），进行大规模组网仿真，模拟大规模的网络业务运行环境，测试人员通过仪器或专有模块，进行多类长周期的测试，推测研判在大规模网络场景中复杂行为可能引起的网络性能和网络安全风险。靶场记录测试过程数据，进行业务模型推演并形成测试结论。

复杂业务安全推演靶场的特点在于自动进行的规模化测试和推演能力。用户基于靶场的靶标库构造特定的仿真程序来模拟或仿真多种特定设备设施、协议或系统。这类设备设施往往成本较高或处于原型阶段，无法进行实体的大规模组网或实验，而复杂业务安全推演靶场的虚拟化和软件定义网络能力和高逼真的仿真技术特点使低成本的实现超大规模的网络建设、数据推演成为了可能。例如，数万个路由器和交换机组成的路由交换网络或由某些特定的物联网设备组成的数万节点的物联网网络等。这些网络的节点均具有相同的协议或功能特点支持靶场平台的快速配置、仿真下发和组网，因此可以利用靶场的核心能力快速完成网络的搭建和反复克隆，在场景构建基础上，基于靶场的数据采集和数据分析能力，利用特定的推演模型和脚本，即可在靶场中低成本和持续的进行仿真推演活动。

复杂业务安全推演靶场通常以软件或软硬件一体化的形式，部署在独立的网络环境中，为客户建设并形成持续的安全推演能力。

公司复杂业务安全推演靶场的典型应用，以某高校物联网推演项目为例。根据合同约定，公司根据安全特征、特种病毒库、特种病毒特征建立一体化的物联网安全检测、监测体系，并搭建一套包含至少三个典型军事场景的军事物联网安全检测和实时监测验证靶场，为物联网应用场景下检测监测验证提供支撑。

利用靶场模拟仿真能力和虚实结合能力，覆盖物联网的“云-管-端”各层面，模拟数千、数万物联网节点遭遇攻击时，对网络的承载能力、异常传播链等特殊情况展开推演研究，形成优化评估指标，有效制定防御方案并持续验证。该案例中推演了数万节点物联网设备被控制以后对供电系统、电力峰值等造成的影响，并在后续的实网演习中得到了验证。



8、综合应用型网络靶场

综合应用型网络靶场是网络靶场中多种应用场景融合的业务形态，发行人基于公司多项关键技术及核心产品构建了虚拟网络仿真场景，结合提炼和总结的国内外重大网络安全事件、众多前沿安全技术及各领域主流网络安全产品等内容，融合多项核心技术形成了多种形态的靶场模块。通过沉浸式和高交互的体验模式，满足各类用户利用网络靶场进行情景式安全教育、实战式人才培养和考核、主流安全产品体验、网络安全演习、重大网络安全事件演练复盘等需求。

综合应用型网络靶场涵盖了公司多种类型和形态的网络靶场，利用网络靶场的底层虚拟化和云技术，以及虚实结合的场景管理和快速下发和资源调度技术，形成了网络教室、网络安全赛场、等你来挑战、数字化展陈等多个展品平台，由于靶场技术的应用，使平台可以快速的进行培训和演练场景的制作、留存和切换，并保证了展品具有极高的稳定性，展品内容易于维护和修改，具有极佳的扩展性和后期升级能力。在展品中将网络安全中的各类知识和技能以场景模板的形态进行快照式的存储，使展品可以满足青少年、普通群众、专业技术人员、企事业单位等各类用户学习和掌握当前国内外最前沿的个人安全、企业安全、数据安全、网络安全等各类知识和案例，用生动形象的视频、知识问答、游戏闯关、实战演练、赛事重现等各种方式使参观者了解网络安全知识、实践网络安全技能，并可以沉浸式的体验网络安全对抗的各种情景。

公司综合应用型靶场业务的典型应用，以网络安全科技馆为例。网络安全科技馆是公司整体负责策划、设计、统筹及建设而成，是 2020 年国家网络安全宣传周的核心场馆，也是“强网杯”全国网络安全挑战赛的永久赛场。作为国内网络安全领域的首个主题馆，网络安全科技馆秉持“聚焦安全、支撑强网、服务产业、助力科普”的建设理念，围绕个人、政企、社会等身边的场景，结合网络靶场系列技术构建而成，属于集赛事演练、人才培养、安全意识教育、安全测试、科学

展示、演练复盘等于一体的综合应用型网络靶场。

三、网络靶场和同行业靶场的区别

(一) 同行业公司

由于同行业公司未详细披露过网络靶场的具体信息，因此无法进行具体比较，但根据数世咨询发布的《网络靶场能力指南》中，共有四家公司提供了网络靶场案例，分别为发行人的“某城市网络靶场建设项目”、南京赛宁提供的“某能源行业用户案例”、安码科技提供的“城市级靶场”、博智安全提供的“某工业网络安全响应中心靶场”，四个靶场对比如下：

序号	公司名称	靶场名称	主要用户价值
1	发行人	某城市网络靶场建设项目	1、城市级场景仿真，覆盖能源、电力、金融、交通、电信等十余个关键信息基础设施行业的超十万网络节点的大规模场景复现，支撑了千人并发任务执行； 2、高仿真验证平台，实现八种角色的多场景任务设定，完成人才培养、攻防演练、测试验证、效能评估等各类任务执行； 3、能够复现安全技术方案及响应方案，结合专业技术团队、技术工具及专业技战法等进行可行性、有效性和相关薄弱环节的安全检验； 4、实现了任务、行业、角色、数据、多架构等的深度融合及全链运营，增强城市全网风险验证能力，打造网络空间“朱日和”基地。
2	南京赛宁	某能源行业用户案例	1、提供各方向的安全课程，并通过大数据精准分析，形成完整的人才能力评价体系，学员通过体系化的学习可快速提高安全技能。 2、提供针对个人、团队业务的多种实网实战演练模式，在虚拟与真实环境中对实际案例进行还原，能培养人员的业务思维、锻炼解决实际问题的能力、积累实战经验、提升团队整体能力以及策略应用。 3、针对网络安全研究人员提供的弹性测试床环境，具有隔离、可控、批量操作、数据自动采集等特性。研究人员可在测试床中开展一系列研究性工作，挖掘系统潜在风险，并对攻防工具进行测评验证。
3	安码科技	城市级靶场	1、通过实网演练，发现重点企业存在的安全风险，及时进行修补。 2、为当地网络安全研究人员提供先进、一流的虚拟环境，满足各种方面的研究需求。 3、基于演练的数据进行分析，进一步形成和丰富网络攻防实验模型和实验数据库，从而提供更高质量的靶场服务。 4、为当地企业提供靶场能力支持，即使其他企业并未购买靶场产品，依然能通过“靶场即服务”的方式，通过靶场能力满足相关的安全需求。
4	博智安全	某工业网络安全响应中心靶场	1、提供包括工控系统攻防场景、卫星导航场景等特殊场景在内的攻防模拟。 2、客户根据自身需求自由构建典型攻防场景。

			3、为客户的员工提供全面的网络安全技术体系课程。 4、基于训练过程数据和结果数据，对人员能力进行分析评估。
--	--	--	--

总体而言，公司网络靶场和同行业网络靶场的作用和目的存在一定的一致性。主要有攻防演练、人才培养、测试验证、效能评估等作用。

（二）鹏城实验室鹏城网络靶场

鹏城网络靶场采用边建边用的模式，实现需求牵引与技术推动并重。成功实践了三种模式的应用。内打内：立足靶场本身，开展网络人才培养和网络对抗演练；内打外：基于网络靶场、面向国家重大网络基础设施和系统，进行实网检测，有效支撑系列“护网”行动；外打内：基于网络靶场，结合外网攻击资源，对重要信息产品进行安全测试，极大提升安全测试的科学性和时效性。

发行人作为鹏城网络靶场的分靶场，发行人网络靶场与鹏城网络靶场功能存在一致性。



鹏城网络靶场合作方较多，主要为四川大学、武汉大学、中科院信工所等高校或科研机构，以及中国联通、宁波国电、南方电网等国家重点基础设施单位，网络安全公司主要为发行人和启明星辰。

发行人已在招股说明书“第六节 业务和技术”之“一、发行人的主营业务、主要产品或服务及设立以来的变化情况”之“（一）发行人的主营业务、主要产品或服务的基本情况 & 收入构成”之“2、主要产品和服务”之“网络靶场系列产品”之“②网络靶场业务场景”补充披露如下：

网络靶场业务的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。根据不同业务场景具体如下：

A、赛事演练靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，人才培养是未来的一大发展目标，要求建成一批网络安全人才实训基地、公共服务平台和实训靶场，创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人才规模质量不断提高。赛事演练靶场正是这一目标下的典型应用场景。

“网络安全的本质在对抗，对抗的本质在攻防两端能力较量。”网络安全赛事可通过网络对抗的模式检验参赛队伍的实战攻防能力和应急协作水平，整个过程需要在专门搭建的、符合行业特征的、安全可控的演练环境中进行，通过竞技形式有效训练选拔网络安全人员。

赛事演练靶场主要采取外打内模式。赛事演练靶场平台提供完备的赛前、赛中、赛后管理功能，支持多种可选的比赛模式、积分计算模式以及配套的多种大屏展示效果。赛事组织方可利用靶场平台自定义赛题或从已有题库和场景库中选择赛题一键下发竞赛，靶场依据策略自动化完成资源管理、数据记录和分析等各类操作。

参赛选手利用分发的账号密码权限登录到靶场平台，获取平台预设好的竞赛靶标进行解题，根据竞赛或演习目的不同，靶标可分为寻找线索类、对抗类、分析类、仿真场景类等多种。同时，平台裁判员也会通过靶场平台对赛事过程进行管理，包括暂停和恢复竞赛、根据平台报警处置违规行为、发布公告及加减分工作等。在举办网络安全赛事时，赛事演练靶场会以软硬件一体的方式部署在赛场或线上，靶场设备独立组网与每一个参赛选手终端联通。

公司赛事演练靶场业务的典型应用，以“巅峰极客”网络安全技能挑战赛为例。根据合同约定，公司负责 2018 “巅峰极客”网络安全技能挑战赛中线下决赛的关键信息基础设施靶场平台定制服务，具体包括：在平台中提供系统管理

模块，供平台系统管理、参数设置、界面管理、人员管理等功能使用；在平台中提供竞赛管理模块，提供全面的竞赛过程管理功能，管理员可对竞赛过程中的竞赛行为进行监控和管理；在平台中提供题目管理模块，管理员可以根据竞赛要求，对竞赛题目模式、类型、数量等进行选择，并对相应题目进行分值设定；在平台中提供竞赛展示模块，主要包括竞赛人员答题界面和竞赛过程展示界面，竞赛裁判或者观众可以通过此界面实时了解各参赛人员的得分情况。

该赛事是中央网信办指导的 2018 年国家网络安全宣传周官方赛事，大赛高度模拟仿真了能源、电力、金融、交通、电信等十余个关键信息基础设施仿真场景，支持 8 种角色在其中进行“真攻真防”技能演练。由渗透测试团队针对虚拟的城市网络体系展开渗透测试；由关键基础设施防御、基础设施业务人员和普通网民、供应链业务系统、网安监管、IT 系统、竞赛裁判及靶场系统运维等 7 个团队组成联合防御队，对抗渗透测试团队对网络的破坏，构筑关键信息基础设施网络系统安全防线。通过赛事演练靶场，一方面检验不同参与角色实战能力；另一方面验证关键信息基础设施和重要信息系统在实战演习演练中的安全防御水平和应急响应能力。

B、人才培养靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，人才培养是未来的一大发展目标，要求建成一批网络安全人才实训基地、公共服务平台和实训靶场，创新型、技能型、实战型人才培养力度显著加大，多层次网络安全人才培养体系更加健全，网络安全人才规模质量不断提高。人才培养靶场正是这一目标下的典型应用场景。

网络安全人才培养需要体系化的课程安排及大量的训练和实践，还需要进行高强度的学习考核计划安排。人才培养靶场就是为人才实践训练和体系化的培养训练专门打造的培训平台。在人才培养靶场平台中，教师和学生分别用自己独立账号登录到靶场，教师在靶场进行教学和考核任务下发，将靶场中自带的课程、实验、题目的学习或考核任务下发给学员，并观察学员培训和考核进展；学员登录到靶场，进行学习和实验训练，也在靶场中进行技能考核。

人才培养靶场是网络靶场的典型应用之一。网络安全攻防对抗具有其特殊性，技能能力的提升必须依赖反复的动手实践才能完成。而网络安全的各类漏洞和

攻防技战法对技能要求的多样性非常高，而网络靶场利用虚拟化和云技术，使各种典型或特定的场景以虚拟机和场景快照模板的方式留存下来，因而可以快速地为人才培养提供各种演练的场景和环境。

在院校或者企业进行人才培养时，人才培养靶场通常以软硬件一体化的方式部署在学校或企业的内网环境，靶场会配置内网 IP 地址，管理员建立和分配教师、学生的账号。教师和学生分别用独立账号登录到靶场。

公司人才培养靶场业务的典型应用，以北京航空航天大学靶场项目为例。根据合同约定，公司提供 e 春秋网络安全实训系统，通过组建专业的网络安全实验室，主要承担信息安全本科专业的教学实验，内容涵盖信息安全专业的主要课程，通过专业设计、创新应用的实验仿真环境，帮助学生可以快速构建实验场景，有效提升学生实践动手的能力。

C、智慧城市安全测试靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，打造网络安全“靶场云”，建设数字孪生靶场，为城市安全能力验证等提供支撑。智慧城市安全测试靶场正是这一目标下的典型应用场景。

在数字化城市的建设过程中，实际上存在大量的数字建设的网络安全风险，在用传统手段发现隐患的同时，还可以通过网络安全测试发现更多风险隐患。在进行安全测试时，测试人员的操作违规或误操作均可能会给系统带来严重的风险隐患，从而导致城市的正常业务运转出现风险。因此业界急需能够对测试人员的测试流程、测试手段等进行标准化和精细化管控，也需要能够在测试中及时辨认和终止这些危险操作并进行自动化的控制，智慧城市安全测试靶场解决了这个难题。

智慧城市安全测试靶场可根据测试组织方的需要为测试团队和人员提供统一的以虚拟机场景为载体的测试操作环境，并使用经过验证和授权的统一链路进行网络安全测试。靶场提供了丰富的操作场景模板库，在每个操作场景中，根据测试任务的需要配置不同的操作系统、经过安全检查和验证的检测工具，防止任何因为测试人员自身的疏忽而将危险的病毒或木马等代入测试目标的情况。操作场景中利用靶场的数据采集技术，对操作行为从操作系统内核、应用以及数据流量等多个层面进行全面行为监控、恶意流量监控，并实时进行屏幕

录像留存，一旦发现危险行为，平台会自动切断网络连接并进行后台报警提示，避免危险的发生。同时，平台将网络安全的服务过程节点化和电子流程化，使每一个安全测试人员的操作均遵循标准的网络安全测试流程和步骤进行，保障安全测试过程和结果的可控可查。

参与测试的人员需要在可控的环境中进行操作，利用与其个人身份绑定的账号权限登录到靶场平台为其独立分配的测试靶场机中，每个账号所使用的测试环境资源均严格隔离，通过靶场机上分配的互联网或内网地址，访问测试目标，检测网络安全风险，测试过程必须在靶场机中完成，靶场会监测测试人员的操作行为，尤其是高风险行为会进行实时的自动报警提示，并赋予管理员阻止非法操作的权限，可设定为自动阻断或人为确定后阻断等。

智慧城市安全测试靶场一般以软硬件一体化的方式部署在互联网或政府指定的内网中。参与测试的安全人员，通过指定的测试账号，接入到靶场中，领取测试任务，并在独立分配的测试靶场机中进行任务操作。

公司智慧城市安全测试靶场业务的典型应用，以广东省数字政府“粤盾”系列测试为例。根据合同约定，公司提供广东省“数字政府”网络安全深度测试服务，为甲方召集并审核技术人才，不定期地对客户指定地“数字政府”政务应用系统开展深度渗透测试，模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，找出未知系统中的脆弱点和未知脆弱点，从攻击者的角度评估，向客户提交发现的安全隐患。通过安全可控的靶场平台中，对相关系统和网站开展“数字政府”网络安全深度测试工作，常态化检验数字政府信息系统安全性。通过累计针对 21 个地市和省直机关数千个重要信息系统开展攻防测试，发现并消除了大量安全隐患。

D、案件线索追踪实战靶场

重点行业在进行案件侦办过程中存在两个比较突出的问题，一是任务人员的工具类型和使用不规范影响任务完成效率，这种状况也使人员的规模化培养以及形成团队战斗力遇到了障碍。二是任务人员自我保护意识和能力不足，容易被目标对象发现从而影响任务效果。

为解决上述问题，使案件线索追踪实战制式化、装备化，并提升自我防护难题，结合客户业务特性和需求研发了案件线索追踪实战靶场。首先，网络靶场

统一管理所有对外链路并形成链路池，可以动态的根据任务要求进行链路的选择或动态切换，统一的链路管理杜绝了被目标发现和反制的风险。其次，统一人员操作环境，凭借网络靶场虚拟机快照和场景库，为各种任务目标和要求准备多样化的标准或定制操作环境，在环境中根据任务要求提供专业规范的工具库，并赋予每个人员独立安全的空间，任务信息及相关关联数据等均根据任务要求实时下发。由于每个人员的操作环境的独立性，任务相关的结果数据和过程数据等均严格隔离，数据的流入和流出均遵循相关安全要求并审计记录，可保障数据安全性。第三，操作环境和操作工具的统一化和制式化，为人才的培训和团队建设等均提供了基础，详实记录的过程数据也使基于靶场平台具备了复盘讲解和总结推演能力，大大提升了团队效率和业务能力。

在进行案件侦办过程中，靶场通过软硬件一体化的方式同时部署在互联网和客户内网。任务管理者可以指定任务的完成人或完成团队，并将任务进行拆解下发，可设定每个任务完成人使用的操作环境及环境中的配套资源和链路，实时查看任务的进度情况进行任务调配等。任务完成人员则利用身份信息和权限登录靶场平台，利用靶场中专门克隆出来的指定操作环境执行相关任务，任务结束后靶场清理和回收资源。

公司案件线索追踪实战靶场业务的典型应用，以公安部门案件线索追踪项目为例。根据合同约定，公司提供复杂网络虚拟化复现及安全演练系统，配置基础网络场景模拟推演靶场装备、一体化作战系统等软硬件产品，仿真网络环境构建、模拟设备，集成主流专用仿真链路场景。可用于攻防任务结束后的案件重演，利用拓扑图结合动画展示渗透路径、防御状态等，对仿真场景中的安全事件进行展示。靶场平台已支撑全国多个省市公安机关开展相关案件追踪活动，开展实战案件侦办。支持公安部及各省、自治区、直辖市公安机关开展了多次的案件实战任务。

E、业务模拟仿真靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，积极推进网络靶场技术研究，建设结合虚拟环境和真实设备的安全孪生试验床，提升网络安全技术产品测试验证能力。国家能源局《关于加强电力行业网络安全工作的指导意见》中提到，建设网络安全仿真验证环境，

适应电力行业网络安全研究、测试、演练等应用需求，整合现有资源，建立覆盖发、输、变、配、用、调度全环节的网络安全仿真验证环境。业务模拟仿真靶场正是这一目标下的典型应用场景。

工业环境对生产系统连续性要求极高，当遭遇网络安全风险时几乎不可能停机进行检修，开展安全测试、技术验证、病毒样本采集分析、模拟风险预警演练等工作，均需要在模拟仿真环境中进行。业务模拟仿真靶场提供了完善的仿真场景构建能力，基于公司多年来积累和沉淀的靶标库和基础场景库、行业仿真场景库等，具备了快速进行行业业务模拟的能力；业务模拟仿真靶场利用模拟仿真的靶场场景提供测试测评、攻防演练、效能评估、科研研发等多种功能。

各个行业的业务存在较大差异，不同的企业或单位的业务网络及应用系统即存在共性也存在各自的特点和特性，而其安全性也相应的具备共性或特性的脆弱点。进行业务模拟仿真，需要利用网络安全的视角了解和分析相关网络的各类要素，并进行提炼和浓缩，将网络安全与业务领域进行融合从而完成仿真和模拟。网络靶场将这些融合的结果沉淀为场景库中的多个场景模板和大量的单机靶标模板。用户可以利用后台功能快速的基于这些基础元素进行调整和定制生成自己企业或单位的仿真场景，并以这些场景来进行各类实训、演练或测试测评活动。

管理者利用账号登录靶场后可进行场景构建、用户管理、任务管理、数据分析、复盘推演或演练测评等各类工作。操作用户则可以在登录靶场后查看被分配的任务、申请场景资源，在场景中完成各种任务并提交数据。靶场支持多任务并发，任务与任务之间数据和资源完全隔离互不干扰，同一任务的不同人员之间可根据任务管理的设定隔离或共享相关资源和环境。不同角色的人员接到各自任务后，在靶场仿真的环境中执行对应的网络安全测试或验证任务。同时，在靶场平台会记录、分析和展示任务的数据、过程和结果。

业务模拟仿真靶场依据用户需要，一般以软件或软硬件一体化方式部署在用户内部网络中。为了达到特定的仿真逼真度，通常会与用户的实体仿真工业设备进行联通。

公司业务模拟仿真靶场的典型应用，以某电网公司网络靶场建设为例。根据合同约定，公司提供网络安全靶场平台及相关能力建设，可实现搭建的虚拟网

络拓扑与实体网络环境进行对接，并构建定制化场景，实现对接实体设备并共同组网。针对电力行业搭建病毒查杀验证靶场环境，选取部分病毒样本，并将病毒样本分别植入行波测距分析系统、数字式电力故障录波装置、故障录波管理机等设备进行查杀测试，持续开展工业仿真场景安全测试验证。

F、人工智能攻防靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，研究人工智能系统可解释性、隐私性等安全要素，突破人工智能模型攻击与防御关键技术，设计实现人工智能系统自动攻防平台，构建人工智能安全靶场。人工智能攻防靶场正是这一目标下的典型应用场景。

人工智能攻防研究是网络安全领域比较前沿的研究方向，需要对人工智能网络攻防对抗有效性和安全性进行研究验证。由于是程序进行自动攻防验证，对于测试目标的资源消耗较大，且会极大影响目标网络性能，甚至会对测试目标的网络造成破坏，需要在安全可控的环境中完成自动测试。靶场提供了安全可靠和灵活的测试环境，还可以自动记录测试参数判断是否达到研制预期效果。用户开发完成人工智能攻防程序后，将程序上传到已经设定好测试环境和靶标的靶场环境中，接到下发的任务指令后，人工智能程序会自动开启攻防测试，靶场中的代理程序也会实时监控环境的稳定性并记录人工智能程序的测试结果是否达到预期目标。人工智能攻防靶场通常以软硬件一体或软件形式部署在独立的网络中，不与用户的办公或生产网络相连。

公司人工智能攻防靶场业务的典型应用，以某自动化测试靶场项目为例。根据合同约定，公司研发一套网络安全领域先进、智能、专业、完善的智能网络攻防比赛系统，即人工智能实验场。依托公司人工智能网络安全靶场平台，将客户自研的人工智能攻防机器人投放在靶场中，对靶场中的靶标进行自动化攻防，通过靶场高柔性的网络环境，在人工智能攻防机器人极具破坏性的测试过程中，确保测试环境的有效性和一致性，并在靶场中实时记录测试数据，统一对人工智能攻防机器人进行效能评估。

G、复杂业务安全推演靶场

工信部《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中指出，积极推进网络靶场技术研究，建设结合虚拟环境和真实设备

的安全孪生试验床，提升网络安全技术产品测试验证能力。国家能源局《关于印发 2021 年电力安全监管重点任务的通知》中要求，推进电力行业网络安全仿真验证环境（靶场）建设，组织开展电力行业网络安全攻防实战演练。复杂业务安全推演靶场正是这一目标下的典型应用场景。

在真实的网络空间中，影响国家安全的网络安全问题通常由多种行为或风险叠加形成，为了预判和风险化解，需要在复杂的大规模推演靶场中利用数字模型和模拟仿真技术等进行仿真推演。进行推演时，靶场管理员登录靶场，在靶场中利用靶场机和专业物理设备（如物联网设备），进行大规模组网仿真，模拟大规模的网络业务运行环境，测试人员通过仪器或专有模块，进行多类长周期的测试，推测研判在大规模网络场景中复杂行为可能引起的网络性能和网络安全风险。靶场记录测试过程数据，进行业务模型推演并形成测试结论。

复杂业务安全推演靶场的特点在于自动进行的规模化测试和推演能力。用户基于靶场的靶标库构造特定的仿真程序来模拟或仿真多种特定设备设施、协议或系统。这类设备设施往往成本较高或处于原型阶段，无法进行实体的大规模组网或实验，而复杂业务安全推演靶场的虚拟化和软件定义网络能力和高逼真的仿真技术特点使低成本的实现超大规模的网络建设、数据推演成为了可能。例如，数万个路由器和交换机组成的路由交换网络或由某些特定的物联网设备组成的数万节点的物联网网络等。这些网络的节点均具有相同的协议或功能特点支持靶场平台的快速配置、仿真下发和组网，因此可以利用靶场的核心能力快速完成网络的搭建和反复克隆，在场景构建基础上，基于靶场的数据采集和数据分析能力，利用特定的推演模型和脚本，即可在靶场中低成本和持续的进行仿真推演活动。

复杂业务安全推演靶场通常以软件或软硬件一体化的形式，部署在独立的网络环境中，为客户建设并形成持续的安全推演能力。

公司复杂业务安全推演靶场的典型应用，以某高校物联网推演项目为例。根据合同约定，公司根据安全特征、特种病毒库、特种病毒特征建立一体化的物联网安全检测、监测体系，并搭建一套包含至少三个典型军事场景的军事物联网安全检测和实时监测验证靶场，为物联网应用场景下检测监测验证提供支撑。

利用靶场模拟仿真能力和虚实结合能力，覆盖物联网的“云-管-端”各层面，模拟数千、数万物联网节点遭遇攻击时，对网络的承载能力、异常传播链等特殊情况进行推演研究，形成优化评估指标，有效制定防御方案并持续验证。该案例中推演了数万节点物联网设备被控制以后对供电系统、电力峰值等造成的影响，并在后续的实网演习中得到了验证。

H、综合应用型网络靶场

综合应用型网络靶场是网络靶场中多种应用场景融合的业务形态，发行人基于公司多项关键技术及核心产品构建了虚拟网络仿真场景，结合提炼和总结的国内外重大网络安全事件、众多前沿安全技术及各领域主流网络安全产品等内容，融合多项核心技术形成了多种形态的靶场模块。通过沉浸式和高交互的体验模式，满足各类用户利用网络靶场进行情景式安全教育、实战式人才培养和考核、主流安全产品体验、网络安全演习、重大网络安全事件演练复盘等需求。

综合应用型网络靶场涵盖了公司多种类型和形态的网络靶场，利用网络靶场的底层虚拟化和云技术，以及虚实结合的场景管理和快速下发和资源调度技术，形成了网络教室、网络安全赛场、等你来挑战、数字化展陈等多个展品平台，由于靶场技术的应用，使平台可以快速的进行培训和演练场景的制作、留存和切换，并保证了展品具有极高的稳定性，展品内容易于维护和修改，具有极佳的扩展性和后期升级能力。在展品中将网络安全中的各类知识和技能以场景模板的形态进行快照式的存储，使展品可以满足青少年、普通群众、专业技术人员、企事业单位等各类用户学习和掌握当前国内外最前沿的个人安全、企业安全、数据安全、网络安全等各类知识和案例，用生动形象的视频、知识问答、游戏闯关、实战演练、赛事重现等各种方式使参观者了解网络安全知识、实践网络安全技能，并可以沉浸式的体验网络安全对抗的各种情景。

公司综合应用型靶场业务的典型应用，以网络安全科技馆为例。网络安全科技馆是公司整体负责策划、设计、统筹及建设而成，是2020年国家网络安全宣传周的核心场馆，也是“强网杯”全国网络安全挑战赛的永久赛场。作为国内网络安全领域的首个主题馆，网络安全科技馆秉持“聚焦安全、支撑强网、服务产业、助力科普”的建设理念，围绕个人、政企、社会等身边的场景，结合

网络靶场系列技术构建而成，属于集赛事演练、人才培养、安全意识教育、安全测试、科学展示、演练复盘等于一体的综合应用型网络靶场。

(2) 区分软件、硬件和服务，分别披露报告期各年度的销售金额及占比情况；

【回复及披露】

发行人已按照软件、硬件和服务，分析报告期各年度的销售金额及占比情况，并在招股说明书“第八节 财务会计信息与管理层分析”之“十、经营成果分析”之“（一）营业收入构成及变动情况分析”之“2、主营业务收入构成情况分析”之“（3）主营业务收入按销售形式分类”处补充披露，补充披露内容如下：

（3）主营业务收入按销售形式分类

报告期内，发行人销售产品收入按销售形式（软件、硬件和服务）分类构成情况如下：

单位：万元

分类	2021 年 1-6 月		2020 年		2019 年		2018 年	
	金额	占比	金额	占比	金额	占比	金额	占比
软件	4,203.39	51.66%	16,061.85	55.07%	7,402.62	45.39%	8,249.11	45.70%
服务	3,238.56	39.80%	10,568.66	36.24%	7,482.48	45.88%	5,022.01	27.82%
硬件	694.13	8.53%	2,533.69	8.69%	1,423.44	8.73%	4,779.91	26.48%
合计	8,136.08	100%	29,164.20	100%	16,308.54	100%	18,051.03	100%

发行人的主营业务收入以软件和服务为主，报告期内，软件和服务收入占比分别为 73.52%、91.27%、91.31%和 91.47%。2018 年硬件收入较高主要系公司承接了南京市公安局、广东省公安厅等公安系统客户的网络安全实验室或靶场建设等一体化建设项目，此类项目中包含实验室及靶场环境建设、硬件设施等需求，因此实验室环境及基础设施建设发生硬件设备收入 2,865.36 万元。2020 年硬件收入较 2019 年有所提高，主要因承接各地公安系统实验室及网络安全平台建设项目发生硬件设备收入 974.70 万元、网络安全科技馆项目发生硬件设备收入 571.79 万元所致。

(3) 剔除网络安全科技馆建设项目影响，公司网络安全产品毛利率逐年下降的原因。

发行人已在招股说明书“第八节 财务会计信息与管理层分析”之“十、经

营成果分析”之“（三）主营业务毛利及其毛利率分析”之“2、主营业务毛利率情况分析”补充披露如下：

报告期内，剔除网络安全科技馆项目后，公司综合毛利率分别为 67.54%、66.69%、63.33%和 56.77%，呈现下降趋势，各业务毛利率如下所示：

分类	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
网络安全产品	57.93%	60.76%	67.57%	66.79%
其中：网络靶场系列产品	58.27%	61.40%	68.76%	65.99%
安全管控与蜜罐产品	65.03%	61.96%	71.68%	71.85%
安全工具类产品	44.86%	58.69%	62.52%	66.90%
网络安全服务	54.14%	67.86%	65.08%	70.16%
其中：安全防护系列服务	52.57%	66.27%	63.11%	69.15%
网络安全竞赛服务	48.76%	61.94%	66.21%	65.79%
其他服务	72.94%	82.00%	71.42%	76.45%
综合毛利率	56.77%	63.33%	66.69%	67.54%

报告期内，公司网络安全产品毛利率分别为 66.79%、67.57%、60.76%和 57.93%，2020 年毛利率较 2019 年下降近 7 个百分点。报告期内，公司处于快速成长期，客户需求逐渐多元，每个项目受到客户所处行业、具体项目类型等因素影响，需要根据客户实际需求进行定制化投入，导致毛利率有所变动，2020 年受泰安市公安局网络靶场系统等项目影响，毛利率有所下降，但是总体而言报告期内毛利率相对稳定。

2020 年毛利率较 2019 年下降近 7 个百分点的主要原因包括：

1、公司政府客户的项目通过招投标方式获取，项目金额受客户预算影响，根据市场竞争情况来考虑报价金额，并非采用成本加成法来确认收入金额。

2、为了争取在具体行业和区域开展业务的机会，以及后续的持续升级维护，公司会承接毛利率偏低的部分项目。例如：公司 2020 年和宁德市公安局签订项目之后，后续又相继签订了宁德市公安局网络安全一体化平台项目、三明市公安局（大田）攻防实验室等业务。

3、低毛利率的项目，依旧体现出公司的核心技术。各主要项目的情况如下：

序号	客户名称	项目名称	收入	毛利率	毛利率下降的原因	核心技术
1	中国信息安全	数据存储与检索系	203.54	44.01%	定制开发存储与检索软件，需要配置相适应	基于单流特征与关联特征相融合的流量检测技术、分

	测评中心	统			高性能存储服务器, 硬件采购成本较高。	布式存储及深度分析技术
2	山西省公安厅	网络平台一期项目	430.09	56.35%	该项目系公安部门一体化项目推行初期所承接, 前期研发成本较高, 毛利率略低。该项目为公司争取到公安系统类似一体化项目的业务机会, 例如贵阳市公安局网络平台(二期)建设项目、河池市公安局网络建设项目(一期)等项目。	面向平行仿真的高性能靶场平台搭建与服务技术、内核级攻击行为全景捕获与复现技术、基于多重隔离的高并发异步靶场构建技术
3	方圆化集团有限公司	武警专修室建设项目	79.65	52.04%	军队行业竞争激烈, 前期拓展市场, 故毛利略低。	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于可扩展元场景的复杂业务模拟技术、基于镜像差分压缩和分级存储的节点快速重构技术、基于多重隔离的高并发异步靶场构建技术
4	国家计算机网络与信息安全管理中心	基于人物关联分析技术研究	81.13	57.10%	在原有产品基础上进行了二次开发, 是空白领域的扩充, 开发成本较高。	智能身份元数据萃取识别技术、基于对抗的非接触高精度溯源反制框架技术、分布式存储及深度分析技术
5	中国银联股份有限公司	2019 年安全攻防竞赛及实训平台建设 IT 软硬件采购合同	66.37	41.28%	该项目覆盖范围广, 用户众多, 支撑软件运行的硬件成本高, 毛利率略低。此外, 该项目也是为了进入银联的战略性项目, 示范效应较高, 公司后续和中国银联陆续签订了 2019 年网络安全演练保障项目、2020 年网络安全培训与竞赛服务等。	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于可扩展元场景的复杂业务模拟技术、基于镜像差分压缩和分级存储的节点快速重构技术、基于多重隔离的高并发异步靶场构建技术
6	泰安市公安局	网络靶场系统采购项目	494.79	27.55%	实验室建设项目需要外采服务器等基础硬件, 毛利率略低。	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于可扩展元场景的复杂业务模拟技术、基于镜像差分压缩和分级存储的节点快速重构技术、基于多重隔离的高并发异步靶场构建技术
7	上海安洵信息技术有限公司	专用设备升级	59.96	31.42%	属于设备升级项目, 成本中包括操作系统远程管理设备、流量卡等硬件, 毛利略低。	基于单流特征与关联特征相融合的流量检测技术、漏洞挖掘及利用验证技术、基于对抗的非接触高精度溯源反制框架技术

剔除掉以上列表项目后,2020 年公司网络安全产品的毛利率为 63.34%。2020 年公司网络安全产品的收入、成本和毛利率具体如下:

单位: 万元

分类	2020 年		
	收入	成本	毛利率
剔除网络安全科技馆项目后的网络安全产品	11,401.32	4,474.42	60.76%
2020 年毛利率偏低的网络安全产品项目	1,415.52	813.27	42.55%
剔除后的网络安全产品项目	9,985.80	3,661.15	63.34%

请发行人说明:

(1) 将网络靶场、人才培养业务列为网络安全产品而非网络安全服务的依据,报告期各期网络靶场业务、人才培养业务(区分线上和线下)的项目数量、收入及占比、毛利率、前五大客户情况;

【回复】

一、将网络靶场系列产品列为网络安全产品的依据、将线上线下培训列为网络安全服务的依据

(一) 主营业务收入构成情况分析

公司的网络靶场应用场景广泛,其中一项应用场景是人才培养靶场,人才培养靶场通常以软硬件一体的方式部署在用户的网络环境中,成为其人才培养、训练、选拔、评价的重要基础平台。公司线上线下培训均依托网络靶场平台进行支撑,利用平台进行教学管理和实验实训等活动。基于网络靶场系列产品和线上线下培训的紧密关系,公司之前将二者进行合并披露。公司的核心业务是网络靶场系列产品,线上线下培训并非公司的核心业务,且报告期内收入占比较低,分别为 5.39%、6.51%、3.24%和 3.97%。

为便于理解公司的主营业务类型及其技术体系,公司对主营业务按照产品与服务维度、技术与应用维度来进行分析。

1、按照产品与服务维度的分类

单位: 万元

二级分类	2021 年 1-6 月		2020 年		2019 年		2018 年	
	收入	占比	收入	占比	收入	占比	收入	占比
网络安全产品	5,656.38	69.52%	22,671.41	77.74%	10,570.16	64.81%	14,012.66	77.63%

其中：网络靶场系列产品	4,825.01	59.30%	18,069.30	61.96%	6,339.87	38.87%	9,954.01	55.14%
安全管控与蜜罐产品	456.18	5.61%	1,565.78	5.37%	1,507.39	9.24%	1,523.45	8.44%
安全工具类产品	375.19	4.61%	3,036.34	10.41%	2,722.89	16.70%	2,535.21	14.04%
网络安全服务	2,479.69	30.48%	6,492.78	22.26%	5,738.38	35.19%	4,038.37	22.37%
其中：安全防护系列服务	1,448.93	17.81%	4,500.82	15.43%	3,867.13	23.71%	2,165.10	11.99%
网络安全竞赛服务	707.43	8.69%	1,046.53	3.59%	809.37	4.96%	899.68	4.98%
其他服务	323.33	3.97%	945.44	3.24%	1,061.87	6.51%	973.59	5.39%
合计	8,136.08	100%	29,164.20	100%	16,308.54	100%	18,051.03	100%

公司为客户提供网络安全产品和网络安全服务。网络安全产品包括网络靶场系列产品、安全管控与蜜罐产品以及安全工具类产品，报告期内的收入分别为14,012.66万元、10,570.16万元、22,671.41万元和5,656.38万元，占比为77.63%、64.81%、77.74%和69.52%。网络安全服务包括安全防护系列服务、网络安全竞赛服务以及其他服务，报告期内的收入分别为4,038.37万元、5,738.38万元、6,492.78万元和2,479.69万元，占比为22.37%、35.19%、22.26%和30.48%。

2、按照技术与应用维度的分类

为了便于理解公司的技术体系，公司对收入按照技术与应用维度进行了分类。网络靶场系列产品、安全管控与蜜罐产品、网络安全竞赛服务主要采用了网络靶场技术，网络靶场技术中应用了平行仿真和攻防技术，对应网络靶场技术下的网络靶场平台、安全管控与蜜罐、网络安全竞赛；安全工具类产品和安全防护系列服务主要应用公司攻防类技术，对应攻防类技术下的专业网络安全服务技术和攻防技术；其他服务列入了其他中。除此之外，对网络靶场系列产品中2020年“网络安全科技馆”项目收入进行了细化分类，将“网络安全科技馆”中与网络靶场技术相关的收入列入网络靶场平台收入，金额为5,923.62万元，其他的收入列入其他中，金额为5,346.47万元，公司根据各个展项使用的技术进行分类。分类金额如下：

单位：万元

分类	2021年1-6月		2020年		2019年		2018年	
	收入	占比	收入	占比	收入	占比	收入	占比
网络靶场技术	5,988.63	73.61%	15,335.13	52.58%	8,656.64	53.08%	12,377.13	68.57%
其中：网络靶场	4,825.01	59.30%	12,722.83	43.62%	6,339.87	38.87%	9,954.01	55.14%

平台								
安全管控与蜜罐	456.18	5.61%	1,565.78	5.37%	1,507.39	9.24%	1,523.45	8.44%
网络安全竞赛	707.43	8.69%	1,046.53	3.59%	809.37	4.96%	899.68	4.98%
攻防类技术	1,824.11	22.42%	7,537.16	25.84%	6,590.02	40.41%	4,700.31	26.04%
其中：专业网络安全服务技术	1,448.93	17.81%	4,500.82	15.43%	3,867.13	23.71%	2,165.10	11.99%
攻防技术	375.19	4.61%	3,036.34	10.41%	2,722.89	16.70%	2,535.21	14.04%
其他	323.33	3.97%	6,291.91	21.57%	1,061.87	6.51%	973.59	5.39%
合计	8,136.08	100%	29,164.20	100%	16,308.54	100%	18,051.03	100%

网络靶场应用“基于混合虚拟化的属性平行仿真技术”“基于靶标分层同步的行为平行仿真技术”“智能身份元数据萃取识别技术”等核心技术，共同解决了高逼真、大规模、对抗性和效能评估问题。从公司产品技术根源上讲，安全管控与蜜罐均是基于网络靶场技术形成，蜜罐重点解决了欺骗式防御产品的高甜度诱捕问题，安全管控重点解决了态势感知产品的高处置问题。网络安全竞赛服务主要依赖于赛事演练网络靶场平台开展业务。网络靶场技术类产品及服务是公司收入的主要来源，报告期占比均超过 50%。

攻防类技术产品主要包括安全防护系列服务和安全工具类产品等。此类产品主要运用了恶意代码检测分析技术、漏洞挖掘及利用验证技术等攻防技术，是公司收入的主要来源之一，报告期内收入金额呈增长趋势，占比分别为 26.04%、40.41%、25.84%和 22.42%。

其他主要包括线上线下培训和网络安全科技馆项目中非网络靶场平台技术展项收入等，报告期内在公司收入中的占比分别为 5.39%、6.51%、21.57%和 3.97%，其中 2020 年网络安全科技馆项目其他收入为 2,858.75 万元。

二、网络靶场系列产品、线上线下培训的业务实质和分类

（一）网络靶场系列产品的业务实质和分类

网络靶场业务的实质是向客户提供软件或软硬件一体化的产品。客户利用网络靶场平台提供的虚拟化仿真场景以及配套的各类应用系统和工具集合来进行赛事演练、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多种业务活动的过程以及其综合应用，作为网络安全基础设施来保障网络安全。

公司的网络靶场系列产品可以根据不同客户的需求,提供不同应用场景的靶场产品。网络靶场系列产品的交付形态为纯软件或软硬件一体化的应用系统和工具集合,提供给客户靶场平台主控中心、春秋云主控中心、靶场平台云计算引擎、靶场平台存储引擎等系统,系统具备场景构建、任务管理、场景运行支撑以及能力分析系统等功能,因此网络靶场系列产品的业务实质是产品。

综合应用型网络靶场是发行人在多个行业、多种技术领域建设网络靶场的综合产品形态,其典型应用场景是网络安全科技馆类产品,如2020年建成的“网络安全科技馆”。综合应用型网络靶场具有综合性特征,一般体现形式为科技馆、演练场等。网络安全科技馆项目中服务收入占比不足20%,产品收入超过80%,业务实质是综合性的网络安全产品。

(二) 线上线下培训的业务实质和分类

报告期内公司的线上线下培训收入占比较低,分别为5.39%、6.51%、3.24%和3.97%。线上和线下培训课程,对学员进行网络安全知识、理念、技能和实践的培训和练习。因此线上线下培训的业务实质是提供培训服务。

三、报告期各期网络靶场业务、人才培养业务(区分线上和线下)的项目数量、收入及占比、毛利率

(一) 网络靶场系列产品、线上线下培训的项目数量、收入及占比

报告期内,发行人网络靶场系列产品、线上线下培训的项目数量、收入及占比如下:

单位:万元

分类	2021年1-6月			2020年		
	项目数量	收入	占比	项目数量	收入	占比
网络靶场系列产品	34	4,825.01	59.30%	63	18,069.30	61.96%
线上线下培训	31	323.33	3.97%	111	945.44	3.24%
其中:线上安全培训	12	50.95	0.63%	41	284.74	0.98%
线下安全培训	19	272.38	3.35%	70	660.70	2.27%

(续上表)

分类	2019年			2018年		
	项目数量	收入	占比	项目数量	收入	占比
网络靶场系列产品	81	6,339.87	38.87%	114	9,954.01	55.14%

线上线下培训	94	1,061.87	6.51%	118	973.59	5.39%
其中：线上安全培训	41	214.99	1.32%	64	137.22	0.76%
线下安全培训	53	846.88	5.19%	54	836.37	4.63%

1、网络靶场系列产品的项目数量、收入及占比

报告期内，发行人网络靶场系列产品的项目数量分别为 114 个、81 个、63 个和 34 个，项目数量逐年减少。网络靶场业务的收入额分别为 9,954.01 万元、6,339.87 万元、18,069.30 万元和 4,825.01 万元，收入先降后升。公司的主营业务收入呈现季节性特征，第四季度收入占比较高，因此 2021 年 1-6 月收入较低。

靶场业务波动的主要原因是 2018 年小项目居多，收入金额在 50 万元以下的项目数量约 70 个。此外，2018 年南京市公安局网络安全实验室建设项目交付验收，该项目确认收入 1,600 余万元，使得 2018 年网络靶场系列产品的项目数量和收入额均处于较高水平。

和 2018 年相比，2019 年靶场业务的项目数量减少 33 个，并且没有 1,000 万元以上的大项目交付验收，使得 2019 年网络靶场系列产品的项目数量和收入额均呈现下降趋势。

和 2019 年相比，2020 年靶场业务的项目数量减少 18 个，主要集中在 20 万元以下的小项目。此外，网络安全科技馆项目确认 11,270.09 万元的收入，昆山九华电子设备厂的基于网络数据处理技术-评估调度子系统项目确认 1,800 余万元的收入，使得当年靶场业务收入上涨。

2、网络靶场系列产品按照应用场景分类的项目数量、收入及占比

单位：万元

应用场景	2021 年 1-6 月			2020 年		
	项目数量	收入	占比	项目数量	收入	占比
赛事演练靶场	2	54.34	1.13%	11	496.74	2.75%
人才培养靶场	12	1,150.64	23.85%	21	561.73	3.11%
智慧城市安全测试靶场	3	873.58	18.11%	3	1,969.26	10.90%
案件线索追踪实战靶场	8	1,751.33	36.30%	14	2,396.06	13.26%
业务模拟仿真靶场	6	729.08	15.11%	5	502.65	2.78%
人工智能攻防靶场	1	61.70	1.28%	4	337.99	1.87%
复杂业务安全推演靶场	1	178.30	3.70%	4	534.77	2.96%
综合应用型网络靶场	1	26.04	0.54%	1	11,270.09	62.37%

合计	34	4,825.01	100%	63	18,069.30	100%
----	----	----------	------	----	-----------	------

(续上表)

应用场景	2019 年			2018 年		
	项目数量	收入	占比	项目数量	收入	占比
赛事演练靶场	8	290.26	4.58%	9	693.05	6.96%
人才培养靶场	39	1,982.34	31.27%	53	1,910.55	19.19%
智慧城市安全测试靶场	5	1,858.29	29.31%	11	384.34	3.86%
案件线索追踪实战靶场	14	555.15	8.76%	29	6,388.01	64.18%
业务模拟仿真靶场	6	430.66	6.79%	7	339.62	3.41%
人工智能攻防靶场	5	577.77	9.11%	2	62.38	0.63%
复杂业务安全推演靶场	4	645.41	10.18%	3	176.06	1.77%
综合应用型网络靶场	-	-	0.00%	-	-	0.00%
合计	81	6,339.87	100%	114	9,954.01	100%

报告期内，发行人网络靶场系列产品的主要应用场景是人才培养靶场、智慧城市安全测试靶场、案件线索追踪实战靶场和综合应用型网络靶场，项目数量每年合计为 93 个、58 个、39 个和 24 个，收入金额每年合计分别为 8,682.90 万元、4,395.78 万元和 16,197.14 万元和 3,801.60 万元，在网络靶场系列产品收入中的合计占比分别为 87.23%、69.34%和 89.64%和 78.79%

3、线上线下培训服务的项目数量、收入及占比

报告期内，发行人线上线下培训的项目数量分别为 118 个、94 个、111 个和 31 个，项目数量先降后升。线上线下培训的收入额分别为 973.59 万元、1,061.87 万元、945.44 万元和 323.33 万元，收入金额保持稳定。

2019 年线上线下培训收入增加 88.28 万元，主要原因是，向大型互联网公司系统的员工销售企安账号进行培训。2020 年线上线下培训收入减少 116.43 万元，主要受新型冠状病毒疫情的影响，认证考试延期或取消，国家网络安全技术认证班业务受到较大影响，导致收入下降。公司的主营业务收入呈现季节性特征，第四季度收入占比较高，因此 2021 年 1-6 月收入较低。

(二) 网络靶场业务、线上线下培训服务（区分线上和线下）的毛利率

报告期内，发行人网络靶场系列产品、线上线下培训服务的毛利率如下：

分类	2021 年 1-6 月	2020 年	2019 年	2018 年
----	--------------	--------	--------	--------

网络靶场系列产品	58.27%	51.41%	68.76%	65.99%
线上线下培训服务	72.94%	82.00%	71.42%	76.45%
其中：线上安全培训	68.54%	92.99%	89.82%	94.41%
线下安全培训	73.77%	77.27%	66.75%	73.51%

报告期内，发行人网络靶场系列产品的毛利率分别为 65.99%、68.76%、51.41% 和 58.27%。公司在前期的研发项目中，积累了大量的软件资源，由于前期研发投入费用化，因此无摊销成本，网络靶场系列产品毛利率稳定在较高水平。2020 年网络靶场系列产品的毛利率下降，主要系网络安全科技馆项目的合同金额较大，涉及部分软硬件外部采购金额较大，从而造成综合应用型网络靶场的毛利率较低。

报告期内，线上安全培训的毛利率分别为 94.41%、89.82%、92.99% 和 68.54%，线上培训的主要成本是云服务器租赁或托管费、课程录制费等，完成录制后可重复售卖和使用，因此该类型业务的毛利率维持在较高水平。2021 年 1-6 月线上安全培训的毛利率为 68.54%，主要是受以下项目的具体影响，具体原因包括定制化网络课程成本较高，线上课程上新和更新的成本较高，以及杭州根本初期项目收入金额较小。剔除掉以下列示项目后，2021 年 1-6 月线上安全培训的毛利率为 89.52%，毛利率基本保持稳定。

客户名称	合同内容	收入	成本	毛利率	毛利率偏低的原因
中国人民解放军	网络课程培训	18.84	8.92	52.68%	该项目提供定制化网络课程培训项目，向客户提供实验环境，进行线上的培训学习和实操演练的成本也较高，因此和标准化课程相比，该项目毛利率偏低。
个人学员	五一嘉峪 2021 年线上 班	7.68	2.72	64.55%	该项目线上课程上新和更新的成本较高，因此毛利率偏低。2021 年公司新上线并更新了部分自身提供的线上课程，2021 年 1-11 月新上线 9 门线上课程，更新 14 门课程，课程前期投入较大，使得毛利率偏低。
个人学员	杭州根本 2021 年线上 班	5.51	2.41	56.29%	杭州根本自 2021 年初开展线上培训业务，初期项目收入金额较小，使得毛利率偏低。
合计		32.04	14.05	56.15%	

报告期内,线下安全培训的毛利率分别为73.51%、66.75%、77.27%和73.77%。线下培训业务的成本中主要包括房租、水电、折旧费、认证考试费、场地费等,因此毛利率低于线上培训的毛利率。2019年的线下安全培训的毛利率减少6.76个百分点,主要原因是当年国家网络安全技术认证班的收入金额较大,认证班目前多与招生渠道合作,需支付场地费、外聘讲师费以及合作分成等,毛利率较低。

四、报告期各期网络靶场业务、人才培养业务的前五大客户情况

(一) 网络靶场系列产品的前五大客户情况

2021年1-6月					
序号	客户名称	收入金额	主要销售内容	应用场景	占收入总额比例
1	中海油信息科技有限公司	1,233.02	网络靶场技术平台研究与应用服务、集团公司综合信息服务、靶场平台仿真环境个性化定制技术服务	智慧城市安全测试靶场、业务模拟仿真靶场、复杂业务安全推演靶场	15.15%
2	河池市公安局	763.19	河池市公安局网络建设项目(一期)	案件线索追踪实战靶场	9.38%
3	网神信息	443.65	企业网络安全人才培养平台V2.0、网络安全攻防业务管理系统V3.0	人才培养靶场、案件线索追踪实战靶场	5.45%
4	大田县公安局	428.14	三明市公安局(大田)攻防实验室	案件线索追踪实战靶场	5.26%
5	厦门安胜网络科技有限公司	383.45	网络安全攻防业务管理系统V3.0、e春秋网络安全实验室靶场系统V3.0、护网行动演练服务	案件线索追踪实战靶场、智慧城市安全测试靶场	4.71%
合计		3,251.45			39.96%
2020年					
序号	客户名称	收入金额	主要销售内容	应用场景	占收入总额比例
1	郑州高新产业投资集团有限公司	11,270.09	郑州高新区网络空间安全科技馆展陈建筑设计装修布展一体化项目	综合应用型网络靶场	38.64%
2	昆山九华电子设备厂	1,886.96	基于网络数据处理技术-评估调度子系统	智慧城市安全测试靶场	6.47%
3	公安部第十一局	813.21	攻防训练资源及培训	案件线索追踪实战靶场	2.79%
4	北京一三一八单位	693.04	联合演练系统升级项目、AI实验场	复杂业务安全推演靶场、人工智能攻防靶场	2.38%

5	泰安市公安局	478.91	网络靶场系统采购项目	案件线索追踪实战靶场	1.64%
合计		15,142.20			51.92%
2019 年					
序号	客户名称	收入金额	主要销售内容	应用场景	占收入总额比例
1	北京市对外服务办公室	1,094.42	平台功能开发及性能优化采购项目	智慧城市安全测试靶场、人工智能攻防靶场、人才培养靶场	6.71%
2	北京华威益腾通讯技术有限公司	838.00	网络安全培训考核仿真平台系统开发	人才培养靶场	5.14%
3	广东省政务服务数据管理局	633.02	广东省政务服务数据管理局 2019 年网络安全体系之靶场及演练培训服务项目	智慧城市安全测试靶场	3.88%
4	北京航天数据股份有限公司	310.00	工业大数据应用技术国家工程实验室（工业大数据人工智能平台）、工业大数据应用技术国家工程实验室（工业大数据基础平台）	人工智能攻防靶场、业务模拟仿真靶场	1.90%
5	石化盈科信息技术有限责任公司	280.48	2019 石化盈科网络安全共享靶场及培训服务中心建设项目软件开发采购及服务合同	人才培养靶场	1.72%
合计		3,155.92			19.35%
2018 年					
序号	客户名称	收入金额	主要销售内容	应用场景	占收入总额比例
1	南京市公安局	1,645.30	网络安全实验室建设项目	案件线索追踪实战靶场	9.11%
2	金鹏电子信息机器有限公司	697.01	广州市公安局网络实验室建设项目	案件线索追踪实战靶场	3.86%
3	安溪县公安局	548.42	网络安全实验室专用设备	案件线索追踪实战靶场	3.04%
4	深圳市公安局网络警察支队	487.00	数据支撑平台项目开发	案件线索追踪实战靶场	2.70%
5	江西省公安厅	384.48	江西省公安厅网安总队实验室专用设备	案件线索追踪实战靶场	2.13%
合计		3,762.21			20.84%

（二）线上安全培训的前五大客户情况

单位：万元

2021 年 1-6 月				
序号	客户名称	收入	主要销售内容	占收入总额比例
1	中国人民解放军 61046 部队训练大队	18.84	网络课程培训	0.23%
2	北京军强致胜教育科技有限公司	2.04	课程授权合同	0.03%
3	江苏开博科技有限公司	2.04	企安殿 i 春秋课程学习培训合同	0.03%
4	深圳市信息安全测评中心	1.26	企安殿在线技术培训服务	0.02%
5	北京谷安天下科技有限公司	0.61	i 春秋优享会员	0.01%
合计		24.79		0.30%
2020 年				
序号	客户名称	收入	主要销售内容	占收入总额比例
1	广东省通信产业服务有限公司广州培训分公司	37.74	2020 年全国行业职业技能竞赛—全国工业互联网安全技术技能大赛赛前集训和选拔（暨网络安全技能培训）	0.13%
2	上海微变信息科技有限公司	18.87	上海税务系统网络安全大比武培训	0.06%
3	甘肃金诺安电子科技有限公司	15.09	CTF&AWD 网络安全竞赛技术培训	0.05%
4	四维创智（北京）科技发展有限公司	15.09	CTF&AWD 网络安全竞赛技术培训	0.05%
5	沈阳世纪中天信息咨询有限公司	9.43	CTF&AWD 网络安全竞赛技术培训	0.03%
合计		96.23		0.33%
2019 年				
序号	客户名称	收入	主要销售内容	占收入总额比例
1	百度时代网络技术（北京）有限公司	37.19	百度全员安全意识培训项目	0.23%
2	中国电信股份有限公司广东分公司	10.34	2019 年广东公司网络安全在线培训项目	0.06%
3	中国人民解放军 68031 部队	9.18	网络技术培训服务	0.06%
4	天津市众思创科技有限公司	8.02	春秋云 SaaS 在线培训合同	0.05%
5	中电科（北京）网络信息安全有限公司	5.90	企安殿在线培训合同	0.04%
合计		70.62		0.43%
2018 年				
序号	客户名称	收入	主要销售内容	占收入总

				额比例
1	国家新闻出版广电总局 监管中心	20.75	网络安全技能实训	0.11%
2	网易（杭州）网络有限 公司	8.51	Web 安全工程师进阶课程合作协议-二 期	0.05%
3	海南政法职业学院	4.72	春秋学堂教学服务（高校版企安殿）	0.03%
4	福建省农村信用社联合 社	4.53	i 春秋企安殿	0.03%
5	江苏江南农村商业银行 股份有限公司	4.34	企安殿 i 春秋线上课程培训服务合同	0.02%
合计		42.85		0.24%

(三) 线下安全培训的前五大客户情况

单位：万元

2021 年 1-6 月				
序号	客户名称	收入 金额	主要销售内容	占收入总 额比例
1	北京信安华宁信息技术 有限公司	96.31	全国网络安全应用检测专业技术人 员（防御方向）委托培训、全国网 络安全应用检测专业技术人员委托培 训	1.18%
2	贵州天网信息科技有限 公司	37.74	贵州电网安全培训与渗透测试服务 项目	0.46%
3	厦门安胜网络科技有限 公司	19.45	培训服务	0.24%
4	石化盈科信息技术有限 责任公司北京分公司	13.96	2020 中国石化总部网络安全管理服 务项目网络安全攻防培训服务合同	0.17%
5	安徽云探索网络科技有 限公司	8.49	培训服务	0.10%
合计		175.95		2.16%
2020 年				
序号	客户名称	收入 金额	主要销售内容	占收入总 额比例
1	北京市对外服务办公室	70.28	网络实战演练技术强化培训合同	0.24%
2	江西神舟信息安全评估 中心有限公司	50.00	网络安全攻防技术培训	0.17%
3	北京信安华宁信息技术 有限公司	39.62	全国网络安全应用检测专业技术人 员攻防赛事专项委托培训	0.14%
4	杭州迪普科技股份有限 公司	31.23	安全技术培训服务	0.11%
5	中央和国家机关涉密载 体销毁中心	18.87	培训服务	0.06%
合计		210.00		0.72%
2019 年				

序号	客户名称	收入金额	主要销售内容	占收入总额比例
1	北京信安华宁信息技术有限公司	208.30	全国网络安全应用检测专业技术人员（防御方向）委托培训、全国网络安全应用检测专业技术人员委托培训	1.28%
2	北京金鸿泰科技有限公司	66.04	网络安全技能实训服务	0.40%
3	中信银行股份有限公司	34.43	信息安全攻防培训、信息安全攻防培训服务、安全开发及意识培训	0.21%
4	公安部第三研究所	28.30	技术培训服务（线下培训）	0.17%
5	北京市凌怡科技有限公司	25.47	网络安全攻防技术培训	0.16%
合计		362.55		2.22%
2018 年				
序号	客户名称	收入金额	主要销售内容	占收入总额比例
1	北京市对外服务办公室第三室	169.81	无线移动高级培训、互联网技术基础培训、第一期网络高级培训	0.94%
2	北京信安华宁信息技术有限公司	158.49	全国网络安全应用检测专业技术人员委托培训（三期）、全国网络安全应用检测专业技术人员委托培训（四期）、全国网络安全应用检测专业技术人员委托培训（二期）、全国网络安全应用检测专业技术人员委托培训	0.88%
3	天津市公安局网络安全保卫总队	90.38	2018 年天津市网络安全人才能力提升培训	0.50%
4	广东省信息技术应用研究所	40.85	课程培训服务	0.23%
5	厦门安胜网络科技有限公司	28.30	网络安全技术培训	0.16%
合计		487.83		2.70%

（2）公司春秋云境网络靶场平台与公司网络靶场业务的关系，是否主要用于支撑网络安全演练活动和人才培养，该平台是如何作为基础设施保障用户网络安全的；

一、春秋云境网络靶场平台与公司网络靶场业务的关系

春秋云境是公司网络靶场系列产品的品牌，网络靶场业务为公司产品类别，公司从事网络靶场业务时以春秋云境为营销品牌。此外，公司还拥有春秋云势、春秋云阵、春秋云盾、春秋云测、春秋云服和春秋云实等品牌，分别对应安全管控、蜜罐、安全工具类产品、安全防护系列服务中的众测服务、其他安全防护系列服务和线上线下培训等产品或服务类别。

二、公司网络靶场及其应用

公司网络靶场应用于多种业务场景，网络安全演练活动和人才培养属于其中两大重要场景，网络靶场应用场景如下表所示：

应用	类别	应用场景	主要体现形式
网 络 靶 场 应用	网络靶场系列产品	赛事演练	产品
		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	
		综合应用型网络靶场	
	安全管控与蜜罐产品	防御监测	单独的防御监测类网络安全产品
	网络安全竞赛服务	安全竞赛	服务

网络靶场系列产品针对不同类型业务和行业客户进行了分类，公司的网络靶场应用场景广泛，支撑客户赛事演练、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多种业务活动的过程及其综合应用。其中赛事演练靶场除提供客户靶场之外，还体现为公司的网络安全竞赛服务。

除此之外，公司利用网络靶场技术研发了安全管控与蜜罐产品，作为网络安全基础设施保障网络安全。蜜罐是网络靶场核心技术的进一步应用，作为单独的防御监测产品形态，蜜罐主要部署于边界安全产品之后，其主要部署在被保护网络内部，与内部网络形成一体，蜜罐和态势感知综合使用下，提高了用户的安全管控能力。

三、公司网络靶场作为基础设施保障用户网络安全的体现

当前我国网络安全建设处于关键阶段，随着云计算、5G、物联网等技术的不断发展，计算机网络的种类和规模均高速增长，网络安全产品和装备的设计研发、测评检验、复杂问题定位及安全推演、方案可行性研究及相关技术的突破均需与之相匹配的科研网络试验环境的支撑，欧美发达国家网络靶场建设均已取得相关成果。

发行人自主研发的“人才培养靶场”和“赛事演练靶场”解决了网络安全实

用型人才培养与评价的难题；研发的“业务模拟仿真靶场”“复杂业务安全推演靶场”和“智慧城市安全测试靶场”解决了政企客户在网络装置原型设计、方案决策、研发测试、测评检验、复杂安全问题定位和推演等过程中网络安全仿真环境缺失的问题；研发的“案件线索追踪实战靶场”为相关用户提供了专业规范的工具库及具有特定属性的专有空间，为客户解决实际业务过程中多维数据整合、数据分析、复盘推演、指挥调度等全过程管理问题；研发的“人工智能攻防靶场”，为人工智能相关技术在网络安全领域的突破融合和实践测试等提供了基础的试验床和数据集，为漏洞挖掘与利用、综合智能攻防等人工智能安全技术的发展及效能验证提供了平台和测试数据集，成为了人工智能技术在网络安全领域实践的有效基础设施。

综合应用型网络靶场是网络靶场多种应用场景融合的综合形态，发行人基于公司多项关键技术及核心产品构建了虚拟网络仿真场景，结合提炼和总结的国内外重大网络安全事件、众多前沿安全技术及各领域主流网络安全产品等内容，融合沙盘建设技术、大数据展示技术、模型构建技术、人机交互技术、动画和视频技术等形成了多种形态的靶场模块，通过沉浸式和高交互的体验模式，满足各类用户利用网络靶场进行情景式安全教育、实战式人才培养和考核、主流安全产品体验、网络安全演习、重大网络安全事件演练复盘等需求。

关于公司网络靶场系列产品的应用场景，请参见本回复报告“2.1、关于网络靶场业务”之“（1）结合具体业务场景，用浅白语言披露公司网络靶场业务的实质、实施方式，所提供产品或服务的具体内容，与同行业网络靶场业务的区别”之“二、不同场景的实施方式以及所提供产品或服务的具体内容”的回复。

（3）网络靶场业务领域的竞争格局、发展趋势，公司在网络靶场领域处于“行业领先地位”的表述依据是否充分。

一、网络靶场的发展趋势

（一）美国网络靶场

根据 2015 年 4 月人民网转发的中国军网的文章《美国网络“曼哈顿计划”》，早在 2008 年，美军就启动了被称为新世纪网络安全“曼哈顿计划”的国家网络靶场建设，为美国国防部模拟真实的网络攻防作战提供虚拟环境。

国家网络靶场是一种测试涉密与非涉密网络项目的国家资源。获得授权进行

测试的组织可与国家网络靶场执行机构协调，安排靶场时间与资源。国家网络靶场为特定试验分配资源，建立试验平台。国家网络靶场支持多任务测试、同步测试、单元测试等。测试工作完成后，国家网络靶场将清理、拆除测试平台，以便靶场回收所用资源。

美国国家网络靶场具有 3 个主要特点：在行业领域，国家网络靶场核心涵盖政府、国防、金融、电信、工业等领域，以满足其网络空间基础设施安全体系建设与科研试验需求；在任务领域，国家网络靶场通过顶层设计与体系建设，完成了网络空间安全体系规划、测试评估、人才教育培养等任务；在应用领域，国家网络靶场可为各类用户提供一系列网络化联合应用，包括支撑国家基础设施安全防护体系建设、自主可控软硬件安全性测试等。

美国建设国家网络靶场引起了各国高度重视。英、德、俄、日、韩等国借鉴美国经验，建设了同类项目，作为支撑网络空间安全技术演示验证、网络武器装备研制试验的重要工具。

2021 年 7 月，据美国国防部网站消息，美国已授权价值 24.10 亿美元的网络靶场相关合同。在未来的 10 年中，赢得订单的公司将为军方网络任务部队提供事件规划和执行、场地安全、信息技术管理以及靶场现代化和作战支持，同时通过测试、规划和系列活动来支持国家网络靶场综合设施的运行。总体上，该合同的主要目标是为其国家网络靶场综合设施提供 IT 服务。

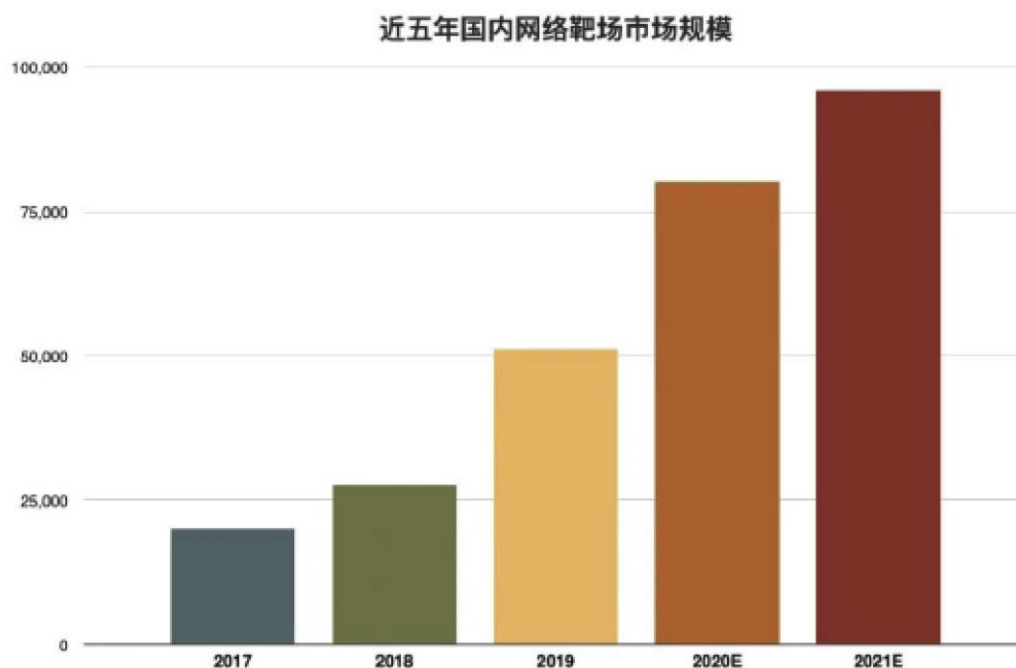
（二）国内网络靶场

我国互联网规模和用户规模均居世界第一，但核心技术与关键资源依赖国外产品情况严重，网络攻击、信息窃取、病毒传播等事件呈多发态势，我国面临的境外网络攻击和威胁越发严重，网络靶场是保障网络安全的重要基础设施。我国网络靶场建设目前处于起步阶段。在国家网络靶场建设方面，无论从靶场基础理论研究、关键技术和产品研发，还是网络空间安全风险评估研究，与欧美国家相比，我国都还存在着一定差距。

随着国家和社会不断加大对网络靶场的投入，贵阳启动大数据网络安全靶场建设、鹏城实验室成立、发行人作为第一完成人的“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获 2019 年度北京市科学技术奖(科学技术进步奖)一等奖、“强网杯”永久赛址郑州网络安全科技馆建立等，网络靶场发展迅速。

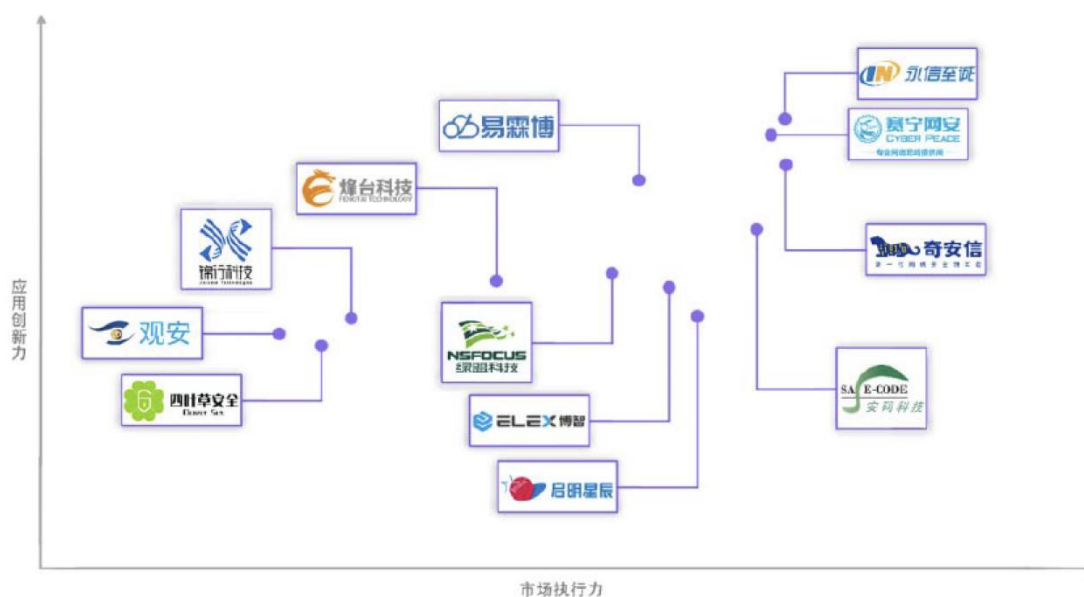
根据 2020 年 7 月份数世咨询发布的《网络靶场能力指南》，近五年网络靶场市场规模如下：

单位：万元



二、网络靶场的竞争格局

根据 2020 年 7 月份数世咨询发布的《网络靶场能力指南》，入选网络靶场能力点阵图的安全厂商有 12 家，分别为：安码科技、博智安全、烽台科技、观安信息、锦行科技、绿盟科技、奇安信、启明星辰、赛宁网安、四叶草、易霖博、发行人。发行人在市场执行力、应用创新力均第一名，具体如下：



三、公司在网络靶场领域处于“行业领先地位”的表述依据是否充分

（一）发行人的产品获得网络安全重要奖项，技术实力得到认可

2018年8月16日公司的网络安全实验室靶场平台获得国家计算机网络应急技术处理协调中心2018年网络安全创新产品（技术）一等奖；2018年9月5日公司网络靶场平台中的网络安全实验室竞赛平台获得中国网络安全产业联盟颁发的网络安全创新产品优秀奖；2019年1月18日公司的网络靶场平台获得中国信息安全杂志社颁发的2018年度中国信息安全产业优秀创新型产品解决方案；2019年9月1日公司的网络靶场平台获得中国网络安全产业联盟颁发的2019年优秀网络安全解决方案和网络安全创新产品。

2018年10月25日，中科合创（北京）科技成果评价中心（科技部有关部门批准成立的全国第一家第三方专业科技成果评价机构）组织院士等专家对公司的“城市网络靶场构建技术及应用”进行集中评定，认定“该项目达到国内领先水平”。公司作为第一完成人的“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获2019年度北京市科学技术奖（科学技术进步奖）一等奖。

（二）发行人技术团队实力突出

公司核心团队主要成员是国内最早的一批网络安全技术专家，拥有十五年以上网络安全从业经历。公司KRLab专注于网络安全创新技术及攻防技术研究，研究内容覆盖操作系统安全技术研究、机器学习与自动化技术研究、Web安全与渗透测试、移动端恶意软件分析、网络蜜罐捕获技术研究等方向。2016年至今，公司团队连续多年参加由公安部主办的国家级网络安全实战攻防演习，曾连续三年企业队排名第一。

（三）发行人居于细分领域领先地位

根据IDC发布的《2020下半年中国IT安全服务市场跟踪报告》显示，永信至诚在IT安全企业级培训服务（包括安全意识培训、安全技能培训、大型赛事、安全靶场等服务）中市场份额为23.35%，位列网络安全行业第一，并已连续四年市场第一；在数世咨询发布的《2020网络安全创新能力100强》中，永信至诚在“攻防技术领域”“仿真技术领域”中均是10强，并获得中国最具发展潜力的年度成长力十强网络安全企业；在数世咨询发布的《网络靶场能力指南》报告中，永信至诚春秋云境网络靶场在应用创新力和市场执行力维度均位列行业第一。

（四）发行人报告期内业务规模不断扩大，重点项目不断落地

公司 2018 年-2020 年实现营业收入分别为 18,051.03 万元、16,308.54 万元和 29,164.20 万元，复合增长率为 27.11%。公司网络靶场及相关技术在多个项目中落地，公司连续两届支持了公安部主导 2018 年开始的两年一届的“网鼎杯”、支持了 2018 年、2020 年、2021 年中央网信办指导的“强网杯”、工信部主办的“全国工业互联网安全技术技能大赛”、信息安全重点实验室主办的“RHG 机器人网络安全大赛”等一系列重大的网络安全赛事和演练活动，在网络安全市场建立了良好的口碑。公司作为牵头方帮助业主方建成了国内第一家以网络安全为主题、以安全意识和科技体验为特色的“网络安全科技馆”，该馆作为 2020 年“国家网络安全宣传周”的核心主场馆。

公司网络靶场在各个地方公安部门落地，比如广东省公安厅、福建省公安厅、云南省公安厅、江西省公安厅、南京市公安局、福州市公安局、杭州市公安局等；还在航天、电力、石油、电信、银行、保险等行业部门落地；以及国际关系学院、哈尔滨工业大学、武汉大学等高校落地。

公司在各地的项目落地可以佐证发行人技术已经具备了较强的竞争力。

【核查程序】

保荐机构执行了以下核查程序：

- 1、访谈发行人核心技术人员及行业专家，了解网络靶场的业务实质和主要目的，了解发行人网络靶场的类别及特点；
- 2、访谈发行人网络靶场产品的主要客户，核实相关产品是否属于网络靶场的真实应用；
- 3、获取发行人主营业务收入明细表，核查发行人主营业务收入按销售形式（软件、硬件和服务）的分类构成情况；
- 4、获取发行人收入成本明细表，核查发行人毛利率变动的原因，分析低毛利率项目的背景；
- 5、获取发行人主营业务收入明细表，核查报告期内网络靶场系列产品和线上线下培训业务的收入构成情况及主要客户情况；
- 6、获取行业研究报告，核查网络靶场业务领域的主要竞争格局，并结合发行人相关指标核查发行人是否具备行业领先地位。

【保荐机构核查意见】

经核查，保荐机构认为：

- 1、发行人网络靶场系列产品符合网络靶场实质；
- 2、发行人网络安全产品毛利率逐年下降具有合理背景，总体而言，报告期内毛利率相对稳定；
- 3、发行人在网络靶场领域具备突出优势，承接重点项目，具备领先地位。

2.2、关于春秋云实人才培养系列产品

根据申报材料：（1）公司 i 春秋线上实训平台主要功能是为政企客户、个人用户提供在线网络安全实验环境，以互联网门户网站形式展现，网络安全技术专家数量超过 700 个，课程超过 316 门，运营的 APP “i 春秋” 平台安装量超过 10 万次；（2）线下安全培训分为线下培训就业班和国家网络安全技术认证班。

请发行人说明：线上、线下培训的盈利模式，网络课程的提供方，相关讲师是否为发行人的员工，发行人该项业务的成本支出构成，收入金额与业务数据的匹配性。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见，说明对发行人线上业务收入的核查情况。

【回复】

请发行人说明：

（1）线上、线下培训的盈利模式，网络课程的提供方，相关讲师是否为发行人的员工，发行人该项业务的成本支出构成，收入金额与业务数据的匹配性。

一、线上、线下培训的盈利模式**（一）线上培训的盈利模式**

线上培训主要以录制课程加提供线上培训实践环境为主，分别为会员制培训、企安殿和网上课程售卖三类。

会员制培训：公司通过 i 春秋网络教育平台网站将公司课程进行整理，客户通过 i 春秋网络教育平台经注册的账号可购买优享会员，进行线上多方向网络安全课程学习。优享会员分为月度会员、季度会员及年度会员三种方式，价格从 100 元到 1,000 元不等。线上会员的成本主要包含带宽费、云服务器租赁或托管费、课程录制费。

企安殿：企安殿平台主要提供给单位用户使用，企安殿账户和个人账号相比多了企业管理员管理功能、竞赛功能和网站视频随意看等功能。一套企安殿的基本产品主要包含 1 个管理员账号和 6 个学员账号，每年的基本服务费用为 5 万元左右。学员账号可以根据客户的培训需求进行增减，每增减一个账号费用随之变动。企安殿的成本主要包含带宽费、云服务器租赁或托管费、课程录制费等。购买企安殿的用户主要为各类大专院校、部队、银行、金融机构、电信及互联网公司，公司通过举办网络赛事和 i 春秋平台网站上宣传企安殿产品，客户根据其需求进行采购。

课程售卖：此板块主要为职业体系化课程业务提供相应的线上课程服务，增加了线上专业助教进行课程管理、学员管理、问答管理等功能，并且可根据客户需求提供定制化的线上培训。公司提供渗透测试工程师课程、CISP-PTE 线上学习课程、CISAW-WEB 安全认证课程、CTF 全方向入门到提高等课程，收费标准在 10,000 元/人/门左右。本板块的主要成本包含带宽费、云服务器租赁或托管费、合作课程分成费、外聘专业助教费等。该类课程主要由 i 春秋网站的注册用户购买，此外包含一些咨询过线下课程，但无法参加面授班的学员购买。

（二）线下培训的盈利模式

线下培训主要包含以下三类培训方式，分别为线下培训就业班、线下培训定制班和线下认证培训班。

线下培训就业班：就业培训通常以线下三个月到四个月的集中面授为主，每次授课班学员在 20 人左右。成本主要包含人工成本、房租、水电、培训平台固定资产折旧费、认证考试费等。就业培训主要面向即将毕业的大学生、待业人员、IT 转安全岗人员、安全爱好者等。公司的招生流量入口为 i 春秋网站、i 春秋公众号、i 春秋 App、老学员介绍和校企合作招生等。

线下培训定制班：该模块是现阶段公司培训业务的主要收入来源，主要包括网络安全技术培训及网络安全大赛技术培训，主要客户类别系政府部门、各大企事业单位、学校等。培训主要为 3-30 天的短期培训。项目培训收费按天计算，根据提供培训的难度不同，按照基础、中级、高级三类难度分别设定收费标准。主要成本包含人工成本、培训场地费、差旅住宿费、外聘讲师劳务费、培训设备运送及实施费等。企业定制化培训业务多为企业客户提供定制开发网络安全产品，

该客户如需进行定制化线下培训则向公司进行采购；同时，公司支撑的网络安全大赛也会给线下培训定制班带来客户。

线下认证培训班：认证培训班系公司线下培训的另外一个重要组成部分。公司作为中国信息安全测评中心、中国网络安全技术审查与认证中心、中国电子科技集团公司第十五研究所等机构的授权培训机构和课程管理机构，有权在中国（包括港澳台）开设培训班，开展信息安全类认证资格培训。认证培训主要针对需要取得专业网络安全认证的人员，开展时长在 5-8 天的培训。主要成本包含人工成本、培训场地费、外派讲师劳务费、差旅住宿费、考试认证费用等。

二、网络课程的提供方，相关讲师是否为发行人的员工

（一）网络课程的提供方

截至 2021 年 12 月 10 日，公司网络课程的提供方情况如下：

单位：门

网络课程的提供方	课程数量	占比
免费课程		
公司	61	17.73%
其他方	152	44.19%
其中：个人讲师	75	21.80%
团体讲师	77	22.38%
小计	213	61.92%
付费课程		
公司	25	7.27%
其他方	106	30.81%
其中：个人讲师	83	24.13%
团体讲师	23	6.69%
小计	131	38.08%
合计	344	100%

公司网络课程包括免费课程和付费课程两大类，课程体系包括基础公开课、知识体系课程和培训认证课程。其中，由公司提供的课程数量占比为 25.00%，公司自行录制的课程主要系 i 春秋实验课程和 i 春秋员工制作的网络安全相关课程。其他方提供的课程数量占比 75.00%，主要是推广类公共知识课程、病毒木马查杀实战、缓冲区溢出分析、密码学基础、网络服务配置与管理等网络安全知

识课程。

（二）相关讲师是否为发行人的员工

1、线上培训的讲师情况

截至 2021 年 12 月 10 日，公司线上培训的讲师情况如下：

单位：门

课程讲师	课程数量	占比
公司员工	86	25.00%
其他方	258	75.00%
合计	344	100%

公司员工制作的课程数量小于其他方制作的课程数量，主要原因系公司为了保证网络安全技术内容的多元化、严谨性和权威性，外聘行业专家、高校教师等专家外购定制化的课程，装载至公司 i 春秋线上实训平台中，根据行业先进经验实时录制并更新课程。

2、线下安全培训的讲师情况

报告期内，公司线下安全培训的讲师情况如下：

单位：天

课程讲师	2021 年 1-6 月		2020 年		2019 年		2018 年	
	课时	占比	课时	占比	课时	占比	课时	占比
公司员工	776	95.21%	600	57.47%	880	67.43%	871	87.45%
外聘员工	39	4.79%	444	42.53%	425	32.57%	125	12.55%
合计	815	100%	1,044	100%	1,305	100%	996	100%

公司线下安全培训的讲师包括公司员工和外聘讲师。报告期内，公司员工提供的线下安全培训的课时占比分别为 87.45%、67.43%、57.47%和 95.21%。公司一般在客户单位所在地开展线下培训业务，考虑到公司自身的讲师数量有限，且长旅途的出差费用较高等因素，公司一般会与当地个人或者团体进行合作。在公司提供网络靶场、培训方案、课程设计等的基础上，由符合资历要求、具备授课经验的培训讲师来开展业务。2021 年 1-6 月，因业务季节性影响，公司项目较少，技术培训人员充裕，上半年线下培训业务多以公司员工讲师为主，同时疫情的反复，也给公司外聘讲师进行线下培训带来不利影响。

三、该项业务的成本支出构成

公司线上线下培训的成本构成情况如下：

单位：万元

项目	2021 年 1-6 月		2020 年		2019 年		2018 年	
	金额	占比	金额	占比	金额	占比	金额	占比
直接人工	34.08	38.96%	53.88	31.66%	103.14	33.98%	62.98	27.47%
外包服务	3.03	3.46%	53.79	31.61%	126.65	41.73%	92.23	40.23%
其他	50.37	57.58%	62.49	36.72%	73.71	24.29%	74.05	32.30%
合计	87.48	100%	170.16	100%	303.50	100%	229.26	100%

公司线上线下培训的成本主要为直接人工和外包服务，报告期内二者合计占比分别为 67.70%、75.71%、63.28%和 42.42%。直接人工主要系项目实施人员的薪酬，是该类业务成本的主要组成部分。外包服务是指项目中涉及的非本公司提供的外包培训等服务，主要包括组织实施培训活动、组织攻防竞赛、师资委派等；其他主要是培训所需要的零星设备、差旅费、会议活动费、场地费、市内交通费等。

四、该项业务收入金额与业务数据的匹配性

公司线上线下培训的收入占比较低，报告期内的收入额分别为 973.59 万元、1,061.87 万元、945.44 万元和 323.33 万元，在当年主营业务收入中的占比分别为 5.39%、6.51%、3.24%和 3.97%。线上线下培训是公司的一种市场营销方式，个人用户增加了公司在网络安全行业的影响力，政企用户加强了公司和客户的商业纽带。

单位：万元

分类	2021 年 1-6 月	2020 年	2019 年	2018 年
	收入	收入	收入	收入
线上安全培训	50.95	284.74	214.99	137.22
线下安全培训	272.38	660.70	846.88	836.37
小计	323.33	945.44	1,061.87	973.59
营业收入总额	8,136.08	29,164.20	16,308.54	18,051.03
占比	3.97%	3.24%	6.51%	5.39%

（一）线上安全培训收入金额与业务数据的匹配性

报告期内，公司线上安全培训的收入构成如下：

单位：万元

分类	2021 年 1-6 月		2020 年		2019 年		2018 年	
	收入	占比	收入	占比	收入	占比	收入	占比
课程售卖	40.16	78.82%	173.52	60.94%	43.38	20.18%	37.38	27.24%
企安殿	3.30	6.47%	78.06	27.41%	131.35	61.10%	64.85	47.26%
会员	7.50	14.71%	33.17	11.65%	40.26	18.73%	34.99	25.50%
合计	50.95	100%	284.74	100%	214.99	100%	137.22	100%

发行人的线上安全培训以课程售卖和企安殿为主，二者报告期的合计收入金额分别 102.23 万元、174.73 万元、251.57 万元和 43.46 万元。2019 年大型互联网企业向公司采购多个企安殿账号，使得公司 2019 年的企安殿收入大幅增加。2020 年受新型冠状病毒疫情的影响，更多客户转向线上培训。此外，公司新增多个行业竞赛的相关培训，使得当年定制化的课程售卖收入大幅增加。

1、课程售卖收入金额与业务数据的匹配性

报告期内，发行人课程售卖的累计课程门数、收入及平均每门课程的收入额如下：

单位：万元

年份	2021 年 1-6 月	2020 年	2019 年	2018 年
累计课程门数	1,040	1,041	1,849	2,604
收入	40.16	173.52	43.38	37.38
平均每门课程的收入	0.04	0.17	0.02	0.01

公司的课程售卖针对个人客户和企业客户的实际需求而设立，将课程门数纳入考虑范围后，报告期内平均每门课程的收入分别为 0.01 万元、0.02 万元、0.17 万元和 0.04 万元。主要原因是 2018 年和 2019 年主要面向个人用户销售课程，平均每门课程的收入在 150-200 元之间。2020 年受新型冠状病毒疫情的影响，更多企业客户转向线上培训，使得当年面向企业客户的定制化课程售卖收入大幅增加，面向企业用户的课程定价也高于个人用户。2021 年 1-6 月公司继续推广企业级客户的定制化课程售卖业务，加强促销活动，导致了课程的销售单价下降。

2、企安殿收入金额与业务数据的匹配性

报告期内，发行人企安殿的项目数量、收入及单个项目平均收入如下：

单位：万元

年份	2021 年 1-6 月	2020 年	2019 年	2018 年
----	--------------	--------	--------	--------

项目数量	2	19	30	32
收入	3.30	78.06	131.35	64.85
单个项目收入	1.65	4.11	4.38	2.03

公司的企安殿平台主要提供给单位用户使用，一套基本的企安殿主要系 1 个管理员账号和 6 个学员账号，每年的基本服务费用为 5 万元左右。由于学员账号可以根据企业员工数增减，每增减一个账号，项目费用随之变动，因此每套企安殿的销售价格可上下浮动。

报告期内企安殿的单个项目平均收入分别为 2.03 万元、4.38 万元、4.11 万元和 1.65 万元。2018 年单个项目的收入额偏低的主要原因是公司承接“春秋学堂”业务，该类业务仅提供学员账号，无需管理员账号，故报价较低，因此 2018 年的单个项目收入额偏低。2019 年大型互联网企业向公司采购多个企安殿账号，使得 2019 年的企安殿收入大幅增加。2019 年和 2020 年每套企安殿的收入额均符合公司的报价政策。

3、会员的收入金额与业务数据的匹配性

报告期内，会员人数、收入及人均收入如下：

单位：万元

年份	2021 年 1-6 月	2020 年	2019 年	2018 年
会员人数	157	701	799	631
收入	7.50	33.17	40.26	34.99
人均收入	0.05	0.05	0.05	0.06

公司的 i 春秋优享会员包括月度会员、季度会员及年度会员三种方式，价格从 100 元到 1,000 元不等。报告期内公司每年销售的优享会员账号分别为 631、799、701 个和 157 个，2018 年至 2020 年销售数量保持稳定，2021 年 1-6 月下降主要系上半年度促销活动及举办安全赛事较少，客户一般会根据赛事举办的情况及促销活动，选择在每年的下半年成为会员。平均每人的培训收入分别为 0.06 万元、0.05 万元、0.05 万元和 0.05 万元，人均收入也符合公司的会员定价政策。

（二）线下安全培训收入金额与业务数据的匹配性

报告期内，公司线下安全培训业务的收入构成如下：

单位：万元

分类	2021 年 1-6 月	2020 年	2019 年	2018 年
----	--------------	--------	--------	--------

	收入	占比	收入	占比	收入	占比	收入	占比
线下培训定制班	95.20	34.95%	430.95	65.23%	363.30	42.90%	494.94	59.18%
线下培训就业班	79.00	29.00%	189.08	28.62%	258.11	30.48%	164.61	19.68%
国家网络安全技术认证班	98.18	36.04%	40.66	6.15%	225.47	26.62%	176.83	21.14%
合计	272.38	100%	660.70	100%	846.88	100%	836.37	100%

发行人的线下安全培训业务以线下培训定制班为主，报告期的收入金额分别为 494.94 万元、363.30 万元、430.95 万元和 95.20 万元，占线下安全培训业务收入的比重分别是 59.18%、42.90%、65.23%和 34.95%。线下培训定制班主要是面向政府部门、各大企事业单位、学校等，提供网络安全技术培训及网络安全大赛技术培训。此外，线下安全培训业务还包括线下培训就业班和少量国家网络安全技术认证班。

2018 年和 2019 年，发行人的线下安全培训业务稳定在 800 万元的收入水平，2020 年受新型冠状病毒疫情的影响，认证考试延期或取消，国家网络安全技术认证班业务受到较大影响，导致线下安全培训业务的收入下降 21.99%。2021 年 1-6 月，受新型冠状病毒疫情的影响，公司线下培训业务班的开设受到一定影响，导致线下培训定制班及线下培训就业班的开设班次及收入均呈下降趋势。

公司的线下培训定制班完全针对客户的实际需求而设立，培训时长从 3 天至 30 天不等，将培训天数纳入考虑范围后，报告期内平均每天的培训收入根据定制班的知识层次和难度不同浮动。

公司的线下培训就业班以三到四个月左右的面授为主，是面向毕业大学生、待业人员、IT 转安全岗人员、安全爱好者等群体的就业导向型培训。2018 年公司线下培训就业班初具规模，2019 年该类项目稳定运行。2020 年公司进行促销推广，对线下培训就业班的价格进行了一定程度的下浮调整，导致 2020 年收入下降。2021 年 1-6 月受新型冠状病毒疫情的影响，公司线下培训就业班的开设受到一定影响，导致该业务当期收入略微下降。

公司的国家网络安全技术认证班主要包括注册网络安全测评专业人员（NSATP）认证培训、注册网络安全渗透评估专业人员（NSATP-A）认证培训等。2018 年和 2019 年，国家网络安全技术认证班的收入金额随着培训人数的增加稳定上升。2020 年受新型冠状病毒疫情的影响，注册网络安全测评专业人员

(NSATP) 认证培训无法按照年初计划准时开通线下班, 全年仅举办了一期攻防专项培训, 其余班次均取消或延迟, 2020 年培训人数大幅减少, 因此国家网络安全技术认证班的培训收入下降。因受新型冠状病毒疫情影响 2020 年度延迟的认证类考试陆续恢复, 2021 年 1-6 月的认证培训类需求增加, 公司该类业务的收入有所增加。

【核查程序】

保荐机构和申报会计师就线上业务收入问题, 履行了以下核查程序:

1、访谈业务总监, 了解公司线上培训的业务模式; 访谈财务总监, 了解公司报告期内的线上培训业务收入的确认政策和收入确认的具体方法, 在报告期内收入确认政策是否保持一贯性; 获取公司销售制度, 检查线上培训业务的相关内控制度, 结合对业务负责人的访谈、线上培训业务的相关测试, 评价公司线上培训业务的内部控制是否健全。

2、访谈业务总监、主要业务人员, 了解公司培训业务的拓展方式、销售模式及销售流程, 评价在项目获取、收入确认、成本归集等方面是否存在异常。

3、访谈业务总监、销售总监, 了解公司报告期内培训业务收入波动的原因; 检查收入成本明细表, 核查报告期各期公司培训业务的培训类型、收入金额、项目数量和占比等, 结合访谈获取的信息进一步分析培训业务收入波动原因, 分析原因的合理性。

4、检查公司的收入成本明细表, 分析培训业务的成本支出情况, 并对大额成本支出进行细节测试; 对外包培训服务的采购合同进行抽查, 结合培训项目情况, 对外包培训服务的讲师数量、讲师资质、采购成本等信息进行核对。

5、获取公司报告期培训业务合同清单、课程销售清单、收入明细表等资料, 比较分析报告期内培训业务收入金额与业务数据的匹配性。

6、对线上线下培训的主要企业客户进行函证, 函证业务是否发生、收入金额是否准确、函证项目具体执行情况。将经确认的项目验收时间与收入确认时点进行比对, 检查收入是否确认至正确期间。

报告期内, 对线上线下培训业务的企业客户执行收入函证的情况如下:

单位: 家、万元

项目	2021年1-6月	2020年	2019年	2018年
----	-----------	-------	-------	-------

线上线下培训-企业客户收入	214.39	706.43	797.37	741.91
发函客户情况				
发函金额	206.96	446.04	583.84	644.45
发函金额占当期线上线下培训-企业客户收入的比例	96.53%	63.14%	73.22%	86.86%
回函客户情况				
回函相符金额	185.54	428.12	540.95	308.34
回函相符金额占发函金额比例	89.65%	95.98%	92.65%	47.84%
回函相符金额占当期线上线下培训-企业客户收入的比例	86.54%	60.60%	67.84%	41.56%
替代性程序验证金额	21.42	17.92	42.89	336.11
回函与替代性程序验证金额占当期线上线下培训-企业客户收入的比例	96.53%	63.14%	73.22%	86.86%
回函与替代性程序验证金额占发函金额的比例	100%	100%	100%	100%

除 2018 年以外，报告期内各期回函相符金额占发函金额比例在 89%以上，占当期线上线下培训-企业客户收入的比例在 60%以上。针对函证回函不符或未回函部分，保荐机构及申报会计师通过获取相关销售合同、项目实施资料、验收单、发票及收款凭证执行替代测试。

7、对培训业务的个人客户抽样执行电话访谈，了解业务背景、交易内容，确认销售业务是否真实发生，检查收入是否符合收入确认条件、是否确认至恰当的会计期间。

报告期内，对线上线下培训业务的个人客户执行电话访谈的情况如下：

单位：家、万元

项目	2021 年 1-6 月	2020 年	2019 年	2018 年
线上线下培训-个人客户收入	108.94	239.01	264.51	231.68
电话访谈确认的收入金额	106.68	177.29	190.13	140.45
核查比例	97.92%	74.18%	71.88%	60.62%

8、获取报告期内公司的资金流水明细，核查线上培训业务的回款信息，复核付款单位、回款金额与收入信息是否匹配。

【核查意见】

经核查，保荐机构和申报会计师认为报告期内公司线上培训业务收入真实、准确、完整。

3、关于网络安全科技馆建设项目

根据申报材料：（1）郑州高新产业投资集团有限公司为发行人 2020 年第一大客户，当年收入金额为 11,270.09 万元，占比为 38.64%，发行人主要承担了该客户网络安全科技馆建设项目；发行人对扣除该项目后发行人 2020 年的盈利情况进行了模拟测算，剔除科技馆项目后，公司 2020 年的收入、利润总额和净利润将出现不同程度的下滑，幅度分别为-38.64%、-105.96%和-106.80%，整体由盈转亏；（2）发行人与合肥探奥作为联合体投标，发行人负责科技馆项目的信息安全展示软硬件展品设计及研发、系统安装及调试、数字化解决方案、展品制作（含购置）、场馆智慧化等工作；（3）在 2020 年 3 月 24 日的投标文件中，双方在项目的投标阶段，粗略预估双方将要承担的工作量比例大致为 75%和 25%，在项目的实际实施过程中，发行人各自所承担的工作内容和投标时的预估发生变化，分配比例为 64.68%和 35.32%。公司享有整个科技馆项目收入总额的 65%，即 12,187.50 万元，其中软件收入、服务收入、多媒体收入和设备收入分别为 7,620.17 万元、2,376.10 万元、1,545.10 万元和 646.13 万元；对应的成本约为 6,100 万元，其中专业技术服务费、设备材料费、其他费用和人工费用分别约为 5,000 万元、700 万元、200 万元和 200 万元；（4）郑州高新智慧城市运营集团有限公司、即刻点石、合肥探奥自动化有限公司和郑州信大现金技术研究院于 2020 年 8 月联合设立郑州天健网安技术有限公司，负责场馆运营，报告期内存在向发行人采购、销售商品的情况。

请发行人说明：（1）结合合同条款、具体施工内容以及采购的高科技展品、展项、硬件设备及展陈系统、组件、第三方软件等与网络安全产品的关联程度，说明网络安全科技馆建设项目与公司主营业务的相关性，与公司原有产品在交付形态上的差异，该项目收入归入网络靶场和人才培养领域的依据；公司对该类业务的规划，是否会持续发生；（2）结合报告期内网络靶场与人才培养业务单个项目收入较低、网络安全科技馆建设项目具有偶发性的特点，以及目前在手订单情况等，说明公司业绩的可持续性，发行人是否持续符合上市标准；（3）网络安全科技馆建设项目的合同主要内容与招投标是否一致，收入金额调整的原因、过程、与工作量的匹配关系，项目验收时点、内容与合同约定的一致性；（4）软件、服务、多媒体、设备收入的划分依据、交付成果，合同中各部分金额的约定情况；发行人在该项目中对外采购的具体内容及主要供应商，专业技术服务费

采购金额较大的原因，发行人实际提供的服务内容，将对外采购部分产生的收入作为核心技术收入的原因；（5）郑州天健网安技术有限公司后续的运营方式，向发行人后续采购的内容。

请保荐机构、申报会计师对上述事项，发行人律师对（1）、（2）事项进行核查，并发表明确意见。

【回复】

请发行人说明：

（1）结合合同条款、具体施工内容以及采购的高科技展品、展项、硬件设备及展陈系统、组件、第三方软件等与网络安全产品的关联程度，说明网络安全科技馆建设项目与公司主营业务的相关性，与公司原有产品在交付形态上的差异，该项目收入归入网络靶场和人才培养领域的依据；公司对该类业务的规划，是否会持续发生；

一、网络安全科技馆项目与公司主营业务的相关性

网络安全科技馆设置个人安全、政企安全、社会安全、综合竞技四个主展区，其中个人安全展区主要部署和应用了公司人才培养靶场，可进行多种人群的网络安全教育培训，展项内容涵盖个人通信安全、个人隐私安全、个人财产安全、家庭空间安全和青少年网络安全等；政企安全展区主要部署公司业务模拟仿真靶场，展项内容包括网站安全、数据安全、专用领域网络安全、智能系统网络安全和网络安全等级保护等；社会安全展区主要应用公司智慧城市安全测试靶场，展项内容包括窃密与反窃密、国家关键信息基础设施安全、供应链安全等；综合竞技展区内容分为赛场和人才培养展区两部分，赛场主要部署公司赛事演练靶场，可承载千人同时进行多场景安全演练，人才培养展区重点设置网络安全人才培养、网络安全竞赛有关内容。网络安全科技馆是 2020 年国家网络安全宣传周的核心场馆，是中央网信办指导的“强网杯”全国网络安全挑战赛的永久赛场。

网络安全科技馆项目属于公司网络靶场系列产品中的综合应用型网络靶场产品，是公司赛事演练靶场、人才培养靶场、业务模拟仿真靶场和智慧城市安全测试靶场的多场景综合性应用，运用了公司网络靶场相关的核心技术。网络安全科技馆项目中直接使用到网络靶场系列产品的展项达 12 项，合计收入金额为 5,923.62 万元，在项目总收入中的占比为 52.56%。

（一）网络安全科技馆项目相关合同约定

根据《郑州高新区网络空间安全科技馆展陈建筑设计装修布展一体化项目合同协议书》，联合体成员的工作内容包括信息安全展示软硬件展品设计及研发，展示初步设计，展品深化设计、制作及安装，系统安装及调试，数字化解决方案，布展设计及施工，以及相关配套服务工作。

信息安全展示硬件部分包括采购的高科技展品、展项、硬件设备、网络设备及相应维护设备。信息安全展示软件设计研发包括开发高科技数字化展陈系统及组件、固化的软件产品、第三方软件产品或中间件、按甲方需求定义设计和（或）二次开发、实施、配置的数字化展陈系统等。

根据《联合体协议书》，联合体各成员单位内部的职责分工如下：发行人负责科技馆项目的信息安全展示软硬件展品设计及研发、系统安装及调试、数字化解决方案、展品制作（含购置）、场馆智慧化等全部工作；合肥探奥负责科技馆项目的展馆初步设计、展示环境深化设计及布展、室内装饰装修工程、展馆内部施工等工作。

根据 2020 年 4 月提交的《郑州网络空间科技馆展陈方案》，经行业内的专家评审和认定，专家同意该展馆设计方案，并出具签字版的《网络空间科技馆建设方案评阅意见》。

从网络安全科技馆项目的最终执行方案和结算清单来看，直接使用到网络靶场系列产品的展项达 12 项，收入金额为 5,923.62 万元，在网络安全科技馆项目收入总额中的占比为 52.56%，和公司的主营业务密切相关。

（二）网络安全科技馆项目的展项情况

1、网络安全科技馆项目的展项与公司主营业务密切相关

从网络安全科技馆的具体展项来看，公司重点建设并提供了网络教室-网安馆专用人才靶场、网络教室-网络安全在线云靶场、网络教室-攻防实战靶场、赛场、数字化展陈等展项。网络安全科技馆项目建设的 164 项展项中，多数与公司主营业务网络安全产品或网络安全服务相关，其中 12 项展项直接运用公司的靶场产品构建，合计金额 5,923.62 万元，占比达 52.56%。

网络科技馆的主要展项（前 12 项）和收入金额如下：

单位：万元

序号	展项名称	归属核心业务类别	展项介绍	收入	占比
1	网络教室-网络安全在线云靶场	网络靶场平台	网络教室内直接部署了公司的人才培养靶场系统,本教室主要面对科技馆对外的云端线上教学能力,在平台中主要添加了链路管理、安全运维管理、资源高可用和一体化调度管理等系统和能力。同时也配置了更多的资源和并发承载能力,可支撑更大规模、更多任务的并发执行。	1,314.20	11.66%
2	赛场	网络靶场平台	赛场基于公司的赛事演练靶场进行设计和研发,除原有靶场的功能外,专门为“强网杯”设计和研发了专有的混合赛制支撑以及全套的展示页面及积分管理系统、靶场秀管理系统等。与场地的多种硬件设置和数据采集节点可完美配合和互动,充分体现了靶场平台在场景构建与设计、平台的兼容性和扩展性、与特定设备的虚实结合、数据采集和自动化行为模拟仿真等方面的价值和优势。	1,251.65	11.11%
3	数字化展陈	网络靶场平台	此展项是网络科技馆的重要安全意识体验展项之一,提供了多种展示内容,涵盖网络安全的多个方面,并设计和实现了与观众互动的多样化互动模式。网络靶场提供了多任务调度和资源管理能力,设置的多种体验软件均以场景包的虚拟机模板形态留存,因此可以统一接口快速的制作、编辑和下发启用。 展项基于公司的赛事演练靶场平台设计和实施,利用了赛事演练靶场可以支持多种演练模式的能力,设置和研发了动漫点播、知识加油站、密码安全度测试、密码泄露检测、安全感测试、CTF 体验、技能比武、意识闯关、安全逃脱等多种演练模式,靶场平台为演练模式中相关演示素材、演练题目等的快速导入和编排替换等提供支持,基于靶场的后台管理页面也可快速的对任意已有模式进行复制、logo 替换、演练过程管理等操作,同时基于演练靶场的数据采集分析和展示能力,可快速对每个演练的历史数据、排行榜等进行查看、调整和重放,大大提升了运维便利性和操作效率,后期新互动模式和子展项的扩充也极为便利且易于编辑,在不添加硬件的情况下具有极佳的扩展性。	1,098.00	9.74%
4	网络教室-网安馆专用人才	网络靶场平台	网络教室内直接部署了公司的人才培养靶场系统,涵盖靶场的春秋云管理系统,靶标库、场景库、工具库、教学库等多种内容资源,支持并发多任务的教学任务管理、班级	911.11	8.08%

序号	展项名称	归属核心业务类别	展项介绍	收入	占比
	培养靶场		管理、教学进度管理、人员自学管理等，支持对教学计划、课程体系、实验场景等进行全面的配置和新建，支持考试管理、自动或手动的考卷管理，支持知识内容与实验内容综合组卷等，可以秒级下发单人自学实验任务，也可以分钟级为百人以下班级统一下发实验资源或组织考试等，对教学过程、自学过程、人员的学习和考试的记录和过程等均可进行以班级为单位或以个人为单位的精细化管理。针对科技馆的科普属性和有针对性的行业教育属性，在此教室平台上，设置了为不同团体、单位和人群甚至包括小学生和社区人群的专有教学实验和课程体系，能够支撑科技馆的各种日常的安全意识或专业技能实训需求。		
5	网络教室-攻防实战靶场	网络靶场平台	本教室基于公司的人才培养靶场，除具有常规的资源管理、数据服务、业务应用等靶场功能之外，强调针对攻防实战技术的各类实验和内容，工具库中部署多种流行的网络攻防工具、特定安全工具集和虚拟设备设施等，培训内容体系和相关的实训演练场景更加逼真和复杂。	552.09	4.90%
6	网络剧场	专业网络安全服务技术	网络剧场展项通过播放影片，以拟人化、故事化的手法，将智能手机的各种系统功能、应用 APP 和网络病毒拟人为一个个角色，建构了一个虚构的网络世界。通过现实世界的人物行为和虚拟网络世界中的人物、事件产生关联，来表现一场网络攻击事件的攻防全过程，从而对观众传播网络安全知识。	405.09	3.59%
7	守护网站安全	专业网络安全服务技术	守护网站安全展项展示省行政区以及若干典型企业的网站安全状态，利用网络、数据、业务、应用、主机、环境等六个维度的数据全面分析和评估网站安全，向观众介绍保障网站安全需要关注的技术和方法，了解网站安全风险、短板的防御手段等，便于理解网站安全的预防策略和部署。	245.19	2.18%
8	等你来挑战	网络靶场平台	此展项是当前国内网多个主流网络安全赛事模式和赛题的融合体验平台。基于公司赛事演练靶场设计，利用靶场中的赛事演练管理能力和赛题库管理能力，将经典的安全大赛真题编排成挑战题目集合，根据挑战活动的难易度选择合适的题目集合进行下发，网络靶场提供完备的赛前、赛中和赛后管理能力，提供针对此展项的展示效果和内容等，并支持在多种赛题模式和积分方式中的快	234.53	2.08%

序号	展项名称	归属核心业务类别	展项介绍	收入	占比
			速切换,靶场的多任务并发能力也可使同一个展品可同时开发多种挑战,增加了展品的弹性和趣味性,并具备较强的升级和扩展能力。		
9	万维之旅	其他技术	万维之旅展项营造一个被三维立体投影画面保卫的完全沉浸式的虚拟环境,置身其中沉浸感强,还可以通过雷达识别手势,与投影画面进行互动,仿佛进入一个若虚若实的网络世界,让参观者在享受一场视觉盛宴的同时,从另一个维度了解网络。启迪人们通过加入万维网,以己之力,聚众之智,共同推动网络文化的繁荣和多态化发展,以创建网络空间命运共同体为指引,共同开创人类发展更加美好的未来。	230.08	2.04%
10	网络安全演练	专业网络安全服务技术	本展项以游戏的形式将常规的安全演练过程制作作为普通观众容易理解的闯关答题模式,参观者通过简单的进行路径方向选项、行为动作选项等来完成闯关,通过播放相关图文和视频等了解演练内容等,从而激发用户对于网络安全的兴趣、提升自我安全意识。	229.20	2.03%
11	我们·网络·世界-点阵空间智慧靶场	网络靶场平台	展现动态的利用点阵的方式控制数百块子屏幕进行运动,在空间中展示相关内容。展品内置多种展示方案,每种展示方案以靶场的虚拟机快照方式进行存储,在快照内存储对应展示方案的 266 个伺服电机参数,参数包括子屏幕的空间位置对应的电机各项参数以及对应子屏幕上的展示内容。靶场利用虚实结合相关技术实现了 Ethercat 网络通讯协议、电力信号转换及电力载波数据传输协议,控制子屏幕的空间位置以及每个子屏的展示内容变换。 基于公司智慧城市安全测试靶场,利用靶场基础平台的虚实结合设备管控系统,设置两百余个管控电机的网络拓扑场景,在场景中设置节点控制系统,利用点阵管理的方式完成对场景中数百个电机的控制。得益于靶场对场景中节点的数据采集、软件定义网络、控制数据投放、场景自检及重置等优势,提升展品的控制能力和容错能力,并可将点阵的初始形态制作成多种场景快照模板在场景数据库中长期留存,快速切换,并支持多任务并行管理能力,具备较好的扩展性和兼容性。	222.27	1.97%
12	时空长	网络	展项以时空走廊的形态引导参观者掌握网	221.58	1.97%

序号	展项名称	归属核心业务类别	展项介绍	收入	占比
	廊-体态互动智慧靶场	靶场平台	络安全性相关的关键信息,并通过行为互动推动时间线变化的体验。网络靶场技术使展项具备了内置多个互动和展示场景的能力,并支持利用行为仿真触发靶场中的自动化攻防脚本推进对应典型场景内的攻防行为,从而触发大屏进行逐步推进的效果展示。内置网安历史沿革场景、典型攻防流程场景、突发安全事件应急处置场景等。 基于公司网络靶场平台,使用公司的场景管理后台模块进行场景和展示效果的统一管理和控制,利用动作行为采集系统实现与场景的交互管控,定制体态识别、容错模块提升识别效率和效果,数字化特效模块完成展示内容的衔接控制。得益于靶场系统的高弹性和扩展能力,场景库中可存储多套不同的展示内容和既定场景组合方案,通过后台的配置进行定时切换、行为触发式切换等,动作识别库中也可设定复杂动作的模型进行精细化动作的快速识别和记录。靶场的任务后台数据管理能力使每种场景的交互动作数量、场景内容切换数量、交互人群数量等均可在后台进行查看、排序和数据统计分析,运维人员可查看最受欢迎的动作、场景内容等,指导后续的展示内容编排和升级。靶场平台的稳定性、易用性和扩展性对展品的运营和使用提供了良好支撑。		
合计				6,914.98	61.36%

在上述展项中,公司利用网络靶场系列产品技术重点支撑了网络教室-网安馆专用人才培养靶场、赛场、数字化展陈、网络教室-网络安全在线云靶场、网络教室-攻防实战靶场、等你来挑战、我们·网络·世界-点阵空间智慧靶场、时空长廊-体态互动智慧靶场共计 8 个展项,合计收入金额为 5,805.42 万元。

从网络安全科技馆的所有展项中来看,公司利用网络靶场系列产品技术重点支撑了网络教室-网安馆专用人才培养靶场、赛场、网络安全知识数字化展陈项展项、网络教室-网络安全在线云靶场、网络教室-攻防实战靶场、等你来挑战、我们·网络·世界-点阵空间智慧靶场、时空长廊-体态互动智慧靶场、生物信息密码、网络安全事件放映厅、我的包裹安全吗和黑客密室共计 12 个展项,合计收入金额为 5,923.62 万元。在网络安全科技馆整体收入中占比为 52.56%,网络

安全科技馆项目和公司的主营业务密切相关。网络安全科技馆的 12 个靶场相关展项具体如下：

单位：万元

序号	展项名称	应用场景	收入	成本	毛利率	展项详情
1	网络教室-网络安全在线云靶场	人才培养靶场	1,314.20	76.36	94.19%	网络教室内直接部署了公司自有的人才培养靶场系统。
2	赛场	赛事演练靶场	1,251.65	67.88	94.58%	赛场基于公司的赛事演练靶场进行设计和研发，除原有靶场的功能外，专门为“强网杯”设计和研发了专有的混合赛制支撑以及全套的展示页面及积分管理系统、靶场秀管理系统等。
3	数字化展陈	赛事演练靶场	1,098.00	655.96	40.26%	展项整体基于公司的赛事演练靶场平台设计和实施，网络靶场作为展项的平台，部分展示内容外部采购，包括意识闯关模块、安全射击模块、安全挑战模块等，由于部分展示内容是外部采购，因此展项毛利率偏低。
4	网络教室-网安馆专用人才培养靶场	人才培养靶场	911.11	60.61	93.35%	网络教室内直接部署了公司的人才培养靶场系统，涵盖靶场的春秋云管理系统，靶标库、场景库、工具库、教学库等多种内容资源，支持并发多任务的教学任务管理、班级管理、教学进度管理、人员自学管理等，支持对教学计划、课程体系、实验场景等进行全面的配置和新建，支持考试管理、自动或手动的考卷管理，支持知识内容与实验内容综合组卷等，可以秒级下发单人自学实验任务，也可以分钟级为百人以下班级统一下发实验资源或组织考试等，对教学过程、自学过程、人员的学习和考试的记录和过程等均可进行以班级为单位或以个人为单位的精细化管理。
5	网络教室-攻防实战靶场	人才培养靶场	552.09	37.45	93.22%	教室基于公司的人才培养靶场，除具有常规的资源管理、数据服务、业务应用等靶场功能之外，强调针对攻防实战技

序号	展项名称	应用场景	收入	成本	毛利率	展项详情
						术的各类实验和内容，工具库中部署多种流行的网络攻防工具、特定安全工具集和虚拟设备设施等，培训内容体系和相关的实训演练场景更加逼真和复杂。
6	等你来挑战	赛事演练靶场	234.53	18.86	91.96%	此展项是当前国内网多个主流网络安全赛事模式和赛题的融合体验平台。基于公司赛事演练靶场设计，利用靶场中的赛事演练管理能力和赛题库管理能力，将经典的安全大赛真题编排成挑战题目集合。
7	我们·网络·世界-点阵空间智慧靶场	智慧城市安全测试靶场	222.27	75.39	66.08%	利用网络靶场平台功能展现动态的利用点阵的方式控制数百块子屏幕进行运动，在空间中展示相关内容。成本主要系外采的全天候循环播放影片制作，视频制作非公司的主营核心业务，因此毛利率稍低。
8	时空长廊-体态互动智慧靶场	智慧城市安全测试靶场	221.58	11.20	94.94%	展项利用网络靶场平台功能以时空走廊的形态引导参观者掌握网络安全性相关的关键信息，并通过行为互动推动时间线变化的体验。
9	生物信息密码	业务模拟仿真靶场	47.84	28.83	39.73%	基于公司综合场景应用靶场，利用靶场的场景复现、模拟交互和数据采集能力，将多种生理特征采集传感器与管控软件系统搭建成为展品场景，利用靶场对场景中各个节点、链路、数据的采集能力，以及靶场对任意节点位置的自动化交互数据投放能力，可以快速高效的控制展品的数据流和每个传感器的启停，模拟出多种密码检测模式，靶场支持将这些模式固化为场景模板等进行长期留存，也支持模板的继承修改、快速自测等，对展品的运营运维、后期调整、动态切换和长期稳定均提供较好的支撑。成本主要系委外制作多媒体动画，视频动画并非公司的主营核心业务，因此毛利率稍低。
10	网络安全事件放映	人才培养	34.75	1.76	94.94%	此展品基于公司人才培养靶场，主要利用了场景管理、课

序号	展项名称	应用场景	收入	成本	毛利率	展项详情
	厅	靶场				程体系管理以及视频播放系统等模块，并定制了相关的交互控制模式，支持对多种视频格式和内容的播放和控制。
11	我的包裹安全吗？	业务模拟仿真靶场	27.06	1.37	94.94%	基于公司业务模拟仿真靶场，模拟城市快递储物箱使用场景，使用了靶场的场景构建系统来设计和规划了快递储物箱个电子操作模块之间的数据传递框架和认证流程，并在场景框架构建起来后，定制开发了快递柜内部的多个仿真业务模块。
12	黑客密室	赛事演练靶场	8.54	0.43	94.94%	基于公司赛事演练靶场设计，利用靶场中的赛事演练管理能力，将春秋争霸、量子幽灵等13道题目植入靶场的赛题库，将展项设置的情节和闯关过程串联起来。
合计			5,923.62	1,036.09	82.51%	

2、网络安全科技馆项目的展项运用了公司的软件著作权、专利以及核心技术

网络安全科技馆在场馆的设计中融合了基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、基于可扩展元场景的复杂业务模拟技术等多个核心技术，公司的多项专利和软件著作权也以具体展项的形式展现出来。8项主要靶场展项和软件著作权、专利以及核心技术的对应关系如下：

序号	展项名称	应用的软件著作权	应用的专利	应用的核心技术
1	网络教室-网络安全在线云靶场	e 春秋网络安全实验室靶场系统 V3.0	一种云平台虚拟资源高速调度方法与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）、一种对等网络应用的监控方法与系统（授权）、一种信息安全竞赛的管理系统及管理方法（授权）、一种网络靶场构建方法系统及存储介质（在审）、一种全要素关联分析方法及装置（在审）、一种关联搜索方法和系统（授权）、城市级网络靶场的 VLAN 划分方法和系统（授权）	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、基于可扩展元场景的复杂业务模拟技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于镜像差分压缩和分级存储的节点快速重构技术、基于多重隔离的高并发异步靶场构建技术
2	赛场	1、网络安全攻	一种云平台虚拟资源高速调度方法	基于混合虚拟化的属

序号	展项名称	应用的软件著作权	应用的专利	应用的核心技术
		防业务管理系统 V3.0 2、网络安全应急响应平台 V1.0 3、网络远程管理系统 V2.0	与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）、一种对等网络应用的监控方法与系统（授权）、一种信息安全竞赛的管理系统及管理方法（授权）、一种全要素关联分析方法及装置（在审）、一种网络靶场构建方法及存储介质（在审）、一种关联搜索方法和系统（授权）、城市级网络靶场的 VLAN 划分方法和系统（授权）	性平行仿真技术、基于靶标分层同步的行为平行仿真技术、基于可扩展元场景的复杂业务模拟技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于镜像差分压缩和分级存储的节点快速重构技术、基于多重隔离的高并发异步靶场构建技术
3	数字化展陈	-	一种云平台虚拟资源高速调度方法与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术
4	网络教室-网安馆专用人才培养靶场	1、网络安全在线教育学习平台 PC 版 V3.0 2、i 春秋信息安全在线教育平台 V1.0 3、企业网络安全人才培养平台 V1.0 4、网络安全竞赛 CTF 个人赛平台 V1.0 5、网络安全竞赛 CTF 团队赛平台 V1.0 6、网络安全人才在线培训认证系统 V1.0 7、网络安全意识学习平台 V1.0	一种云平台虚拟资源高速调度方法与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）、一种对等网络应用的监控方法与系统（授权）、一种信息安全竞赛的管理系统及管理方法（授权）、一种全要素关联分析方法及装置（在审）、一种网络靶场构建方法及存储介质（在审）、一种关联搜索方法和系统（授权）、城市级网络靶场的 VLAN 划分方法和系统（授权）	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、基于可扩展元场景的复杂业务模拟技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于镜像差分压缩和分级存储的节点快速重构技术、基于多重隔离的高并发异步靶场构建技术
5	网络教室-攻防实战靶场	1、Web 漏洞挖掘系统 V2.0 2、安卓安全检测系统 V2.0 3、安卓木马样本主动获取与综合分析系统 V2.0 4、网络安全单兵工具箱系统 V2.0	一种云平台虚拟资源高速调度方法与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）、一种对等网络应用的监控方法与系统（授权）、一种信息安全竞赛的管理系统及管理方法（授权）、一种网络靶场构建方法及存储介质（在审）、一种全要素关联分析方法及装置（在审）、一种关联搜索方法和系统（授权）、城市级网络靶场的 VLAN 划分方法和系统（授权）	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术、基于可扩展元场景的复杂业务模拟技术、面向平行仿真的高性能靶场平台搭建与服务技术、基于镜像差分压缩和分级存储的节点快速重构技术、基

序号	展项名称	应用的软件著作权	应用的专利	应用的核心技术
		5、Linux 安全检查工具软件 V2.6		于多重隔离的高并发异步靶场构建技术
6	等你来挑战	-	一种云平台虚拟资源高速调度方法与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）	基于混合虚拟化的属性平行仿真技术、基于靶标分层同步的行为平行仿真技术
7	我们网络世界-点阵空间智慧靶场	-	一种云平台虚拟资源高速调度方法与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）	基于靶标分层同步的行为平行仿真技术
8	时空长廊-体态互动智慧靶场	-	一种云平台虚拟资源高速调度方法与系统（授权）、网络靶场场景描述文件的生成方法和装置（在审）	基于靶标分层同步的行为平行仿真技术

（三）网络安全科技馆项目采用总额法确认收入的依据

网络安全科技馆共设置 164 个展项，公司合计参与 128 个展项的设计和制作，其余 36 个展项完全由联合体成员合肥探奥承担。公司参与的 128 个展项中，直接使用到网络靶场系列产品的展项达 12 项，合计收入金额为 5,923.62 万元，占公司网络安全科技馆项目收入比例为 52.56%。非公司网络靶场相关的展项达 116 项，合计收入金额为 5,346.47 万元，占公司网络安全科技馆项目收入比例为 47.44%。

非公司网络靶场相关的展项中，存在 84 个展项不涉及公司的自研软件和自制多媒体，主要通过外采完成，包括外购设备、软件和多媒体，该部分展项的收入金额为 3,748.23 万元，在网络安全科技馆整体收入中占比为 33.26%。公司自制和外采结合完成的展项为 11 项，该部分展项的收入金额为 1,334.78 万元，在网络安全科技馆整体收入中占比为 11.84%。公司完全自制的展项为 21 项，展项内容全部是公司的自研软件和自制多媒体，该部分展项的收入金额为 263.46 万元，在网络安全科技馆整体收入中占比为 2.34%。各类型展项的具体情况如下：

单位：万元

展项类别	展项数量	收入					成本	毛利率	记入核心技术的收入额	公司承担的主要工作
		软件收入	服务收入	多媒体收入	设备收入	收入合计				
网络靶场类展项	12	4,921.71	700.78	240.57	60.56	5,923.62	1,036.09	82.51%	5,923.62	多场景综合性应用公司赛事演练靶场、人才培养靶场、业务模拟仿真靶场和智慧城市安全测试靶场,运用了公司网络靶场相关的核心技术。
其他技术类展项	116	2,104.91	1,514.69	1,217.08	509.80	5,346.47	5,118.60	4.26%	-	
其中：委托制作	84	1,918.68	466.70	858.49	504.37	3,748.23	3,832.76	-2.26%	-	在公司的设计思路和理念的指导下,形成包含软硬件展品设计及研发、系统安装及调试、数字化解决方案、展品制作(含购置)、场馆智慧化等环节的一体化解决方案。并且对委外制作部分的内容描述、硬件指标等进行明确要求,向供应商采购非标准化产品。
公司自制加外采	11	159.02	1,017.68	152.64	5.43	1,334.78	1,272.51	4.66%	-	在公司规划和设计思想的指导下,结合自制软件、自制多媒体、委托制作多媒体等多种方式,将软件 and 多媒体灌装到硬件设备中。
公司自制	21	27.21	30.31	205.94	-	263.46	13.32	94.94%	-	公司对展项进行设计和规划后,完全独立制作软件和多媒体来呈现。
合肥探奥承担的展项	36					-	-	-	-	
总计	164	7,026.62	2,215.46	1,457.64	570.36	11,270.09	6,154.68	45.39%	5,923.62	

(续)

单位：万元

展项类别	展项数量	硬件设备采购金额	多媒体视频采购金额	软件及技术服务采购金额	合计	采购内容
网络靶场类展项	12	56.44	90.57	636.29	783.29	硬件设备：服务器、台式机、显示器、触控一体机等，作为软件和系统的载体； 多媒体视频：多媒体视频，支撑了展项的可视化呈现； 软件及技术服务：在线影音互动答题系统部分模块，在数字化展陈展项中，使用公司网络靶场平台作为基础，搭建了自制的动漫点播、密码安全检测等系统模块与外购的在线影音互动答题系统模块，通过系统不同模块带给游客交互式体验效果。
其他技术类展项	116	713.40	971.51	3,194.98	4,879.89	-
其中：委托制作	84	528.32	868.68	2,275.81	3,672.80	硬件设备：电视、量子学习机、服务器、交换机等，作为软件和系统的载体； 多媒体视频：多媒体视频，支撑了展项的可视化呈现； 软件及技术服务：展项的各类软件开发，在 APT 攻击态势、信息隐藏与重现等展项中，游客通过公司采购的 APT 可视化系统、信息隐藏互动系统、网站密码盗取体验系统等，交互式体验 APT 攻击、信息泄露、密码盗取等日常生活中的网络风险。
公司自制 加外采	11	185.08	102.83	919.17	1,207.08	硬件设备：手机、拼接屏、展示桌椅等，作为软件和系统的载体； 多媒体视频：多媒体视频，支撑了展项的可视化呈现； 软件及技术服务：触控系统、装修设计等，使展项更美观地呈现给游客，触控系统可以提升游览过程的直观感受，达到交互式体验效果。
公司自制	21	-	-	-	-	-
合肥探奥 承担的展项	36	-	-	-	-	-
总计	164	769.84	1,062.08	3,831.26	5,663.18	-

公司与郑州高新产业投资集团有限公司签订的《郑州高新区网络安全科技馆展陈建筑设计装修布展一体化项目合同协议书》系为独立的购销合同，不属于中国证监会《首发业务若干问题解答（2020年6月修订）》问题32中提到的委托加工业务合同。同时，公司对网络安全科技馆项目采用总额法确认收入，符合合同实质、公司承担的工作内容和《企业会计准则第14号——收入》的相关

要求。公司承担向客户转让商品的主要责任，在转让商品之前或之后承担了该商品的存货风险，有权自主决定所交易商品的价格，是网络安全科技馆项目的主要责任人。

网络安全科技馆项目采用总额法确认收入的主要原因如下：

1、根据《联合体协议书》，公司负责“科技馆项目的信息安全展示软硬件展品设计及研发、系统安装及调试、数字化解决方案、展品制作（含购置）、场馆智慧化等全部工作”，公司负责向客户提供科技馆的一体化解决方案。

2、公司负责网络安全科技馆项目的整体展馆规划和设计工作，所有展项都是公司网络安全思想和理念的具体体现。采购合同中也明确约定“在展品设计和展品制作（含购置）具体实施过程中，每个阶段的实施方案均需按照甲方、最终用户及其组织的专家评审意见进行修改完善”，合同附件中清晰列示出展项的名称、内容描述、硬件指标等要求。因此外采的展项也是在公司的设计思路和理念的指导下进行采购的非标准化产品。

3、公司负责网络安全科技馆项目的设计、监制、验收、实施和运营工作，公司对每一个展项均组织开展验收工作，公司是所有展项的主要责任人。

4、公司对网络安全科技馆项目采用总额法确认收入符合《首发业务若干问题解答（2020年6月修订）》问题32中的相关规定

（1）公司签署的合同属性类别是独立购销业务

根据《联合体协议书》，公司负责“科技馆项目的信息安全展示软硬件展品设计及研发、系统安装及调试、数字化解决方案、展品制作（含购置）、场馆智慧化等全部工作”。合同中明确约定了合同总价款，该价格属于固定总价，价格本身不区分材料采购价格及留存利润。

合同中明确约定存货转移风险归属的规定“未通过竣工验收的展品展项，其货物风险由公司承担”，公司已验收的材料或者产品在项目整体竣工验收前，由公司承担风险，待项目整体竣工验收后，货物的风险方进行转移。

（2）公司承担了项目建设中存货的保管和灭失、价格波动等风险

公司与郑州高新产业投资集团有限公司、各供应商分别单独签订销售和采购的商业合同，公司与郑州高新产业投资集团有限公司签订的合同中明确约定公司在“设计制作全过程方面、工期延误方面、工程质量方面、项目分包、转包安全

生产方面等的全部违约责任”，公司是网络安全科技馆项目的主要责任人。同时，供应商及存货价格系由公司根据项目需求及市场状况自行选择及自主定价，而销售价格则参照公司及联合体向客户提交的中标方案及《郑州高新区网络空间安全科技馆展陈建筑设计装修布展一体化项目合同协议书》中的约定价格执行，存货采购的价格不随销售价格变动而变动，公司承担了采购材料的价格变动风险。采购的材料到货后，公司需先对采购存货进行验收，取得采购存货所有权，承担存货减值和毁损灭失风险。

（3）公司具备对最终产品的完整销售定价权

公司的项目整体价格均为公司及联合体联合做出，公司及联合体向客户提交的中标方案及《郑州高新区网络空间安全科技馆展陈建筑设计装修布展一体化项目合同协议书》中的约定价格已包含所有硬件成本、软件成本及分包成本，公司及联合体对最终产品具有完整定价权。

（4）公司承担了最终产品销售对应账款的信用风险

公司根据网络安全科技馆项目的实际需求选择多个不同的供应商，公司与郑州高新产业投资集团按照合同的约定金额及付款进度独立结算合同价款，与公司是否向供应商结算采购款的进度及金额无关。公司基于每个供应商各自的供货进度及产品质量，按照采购合同的相关约定进行付款。公司的销售收款进度与公司的采购付款进度无匹配关系。公司承担了最终产品销售的全部信用风险。

（5）外部采购产品在整体交付时经过了系统加工，产品的功能、形态等各方面发生了实质性变化

网络安全科技馆项目建设复杂程度高，在项目整体竣工验收时采购的产品在形态、功能等方面发生较大的实质性变化。

公司网络安全科技馆展项的采购是基于公司靶场平台等公司深耕领域，将每个展项以大众容易接受的方式进行设计和研发，并根据经过设计之后所需展示的硬件需求、多媒体制作需求及分包需求寻找合适的供应商进行外包。外包完成后，公司再将进行进一步灌装，并将公司自行研发部分与外包部分进行软硬结合，制作为方便大众所接受的网络安全领域展项，经过上述工序后，公司的展项从形态上、功能上与直接采购内容相比已发生实质变化。

5、根据《企业会计准则第 14 号——收入》的相关要求，公司对网络安全科

科技馆项目采用总额法确认收入符合《企业会计准则》相关规定。

根据《企业会计准则第 14 号——收入》第三十四条，企业应当根据其在向客户转让商品前是否拥有对该商品的控制权来判断其从事交易时的身份是主要责任人还是代理人。企业在向客户转让商品前能够控制该商品的，该企业为主要责任人，应当按照已收或应收对价总额确认收入；否则该企业为代理人，应当按照预期有权收取的佣金或手续费的金额确认收入，该金额应当按照已收或应收对价总额扣除应支付给其他相关方的价款后的净额或者按照既定的佣金金额或比例等确定。

企业向客户转让商品前能够控制该商品的情形包括：

（1）企业自第三方取得商品或其他资产控制权后再转让给客户

公司从供应商处购买硬件设备、多媒体以及软件后，由供应商运送至公司约定或指定的地点，公司会对硬件等设备进行签收。由供应商提供电子文件光盘的，会采用测试的方式进行验收，并出具技术项目验收证明。部分软件系统或服务会直接部署在公司的服务器上。公司取得了商品的控制权后，再转让给郑州高新产业投资集团有限公司。

（2）企业能够主导第三方代表本企业向客户提供服务

①在网络安全科技馆项目的实际执行过程中，公司利用自身的核心技术和专业能力，对软硬件产品进行一系列的测试、调整、优化和适配，以满足客户的整体需求，提供包括信息安全展示软硬件展品设计及研发、展示初步设计、展品深化设计、制作及安装、系统安装及调试、数字化解决方案等环节的一体化解决方案。

②公司分别与客户签订销售合同，与供应商签订采购合同，采购交易和销售交易相互独立，不存在客户指定供应商采购的情形。

③虽然部分硬件产品由供应商直接发货到网络安全科技馆，但该行为也是由公司协调供应商和客户建立联系，并要求供应商按照采购合同约定的发货品类、数量、规格，到公司指定的收货地点进行交货。

④若客户在产品使用过程中出现产品质量问题，根据合同约定，将由公司承担“制作全过程方面、工期延误方面、工程质量方面、项目分包、转包安全生产方面的等全部违约责任”。

上述情况均表明公司能够主导第三方代表本企业向客户提供相关服务。

(3) 企业自第三方取得商品控制权后，通过提供重大的服务将该商品与其他商品整合成某组合产出转让给客户

为满足客户对科技馆的整体需求，公司交付的展项并非将相关软件和硬件简单组装，而是利用自身的核心技术和专业能力，对软硬件产品、多媒体等进行一系列的测试、调整、优化和适配，提供包括信息安全展示软硬件展品设计及研发、展示初步设计、展品深化设计、制作及安装、系统安装及调试、数字化解决方案等环节的一体化解决方案。

公司从供应商处购买硬件设备、多媒体以及软件并验收后，需要灌装到硬件设备上，并且和公司的自有软件、自制多媒体等结合起来，整合成完整的展项形态，以网络安全科技馆整体展馆的形态提供给客户。

在具体判断向客户转让商品前是否拥有对该商品的控制权时，企业不应仅局限于合同的法律形式，而应当综合考虑所有相关事实和情况这些事实和情况包括：

(1) 公司承担向客户转让商品的主要责任

公司与郑州高新产业投资集团有限公司、供应商分别签订商业合同，合同中均已明确约定了各自的权利及义务，公司负责网络安全科技馆项目的设计、监制、验收、实施和运营工作，公司对每一个展项承担“设计制作全过程方面、工期延误方面、工程质量方面、项目分包、转包安全生产方面的等全部违约责任”。公司与客户、供应商三方之间的责任义务能够区分，公司承担向客户转让商品的主要责任，是网络安全科技馆项目的主要责任人。

(2) 公司在转让商品之前或之后承担了该商品的存货风险

供应商将采购合同约定的产品和服务交付给公司后，采购合同中的主要义务已履行完毕，产品和服务的主要风险已转移给公司。科技馆项目合同中明确约定“未通过竣工验收的展品展项，其货物风险由公司承担”，公司是销售业务的主要责任人。

(3) 公司有权自主决定所交易的商品和服务的价格

公司有权自主选择供应商，可独立外购对应展项产品的采购选择和安排，包括供应商选择、采购数量、价格、结算条款等，并根据合同条款“经监理公司确认后方可进行采购，并由监理保留样品。材料进场前，必须经过监理公司的检查。

监理单位同意后，方可进场”。

公司与郑州高新产业投资集团有限公司、各供应商分别签订商业合同，合同中均已明确约定了各自的权利及义务，公司是主要的义务人，负有向郑州高新产业投资集团有限公司提供商品或服务的主要责任，包括确保所提供的商品或服务可以被客户接受。公司能够自主决定所交易的商品和服务的价格，网络安全科技馆项目的合同金额由公司和郑州高新产业投资集团有限公司协商确定，与公司向上游供应商的采购价格无关。在公司与客户确定产品价格后，采购价格不随公司对客户的销售价格变动而变动，公司承担了相关产品价格波动的风险。

（4）公司承担了信用风险

公司根据网络安全科技馆项目的实际需求选择多个不同的供应商，公司与网络安全科技馆独立结算销售价款，独立结算采购款，公司根据每个供应商各自的供货进度进行付款，销售收款进度与采购付款进度无匹配关系。

综上，公司向郑州高新产业投资集团有限公司交付网络安全科技馆的项目整体产品和服务，就项目整体自主向客户进行报价，同时公司在满足客户整体项目性能的基础上自主选择供应商、自主与供应商约定产品价格，公司是网络安全科技馆项目的主要责任人并承担供应商交货后的存货风险、客户的信用风险，公司在该交易中的身份为主要责任人。销售收款进度与采购付款进度无匹配关系。公司采用总额法确认收入的依据充分的，符合《企业会计准则》的相关规定。

二、网络安全科技馆项目与公司原有产品在交付形态上的差异

网络安全科技馆项目与公司其他网络安全产品在交付形态上均主要表现为纯软件或软硬件一体化产品。

公司原有的春秋云境网络靶场平台在交付形态上表现为纯软件或软硬件一体化产品。软件功能包含场景构建、任务管理、统一认证、春秋云平台、场景运行支撑、能力分析系统、靶标资源包等，硬件系统包括靶场平台主控中心、春秋云主控中心、靶场平台云计算引擎、靶场平台存储引擎、靶场平台存储交换机等。

网络安全科技馆属于公司的综合应用型网络靶场，是公司赛事演练靶场、人才培养靶场、业务模拟仿真靶场和智慧城市安全测试靶场的多场景综合性应用，在交付形态上主要表现为纯软件或软硬件一体化产品，具体包括软件、软硬件一体化、多媒体及设备，共计 164 套展项。

网络安全科技馆中主要展项的交付内容和交付形态具体如下：

序号	展项名称	交付内容	交付形态
1	网络教室-网络安全在线云靶场	根据不同群体和安全角色打造一间网络教室，布置桌椅、电脑、大屏幕等基础硬件设施外，部署一套春秋云境网络靶场平台系统，其中六大子系统：虚拟仿真分系统、比武竞赛分系统、安全实训分系统、综合管理分系统、软件资源包、精品课程定制。内容涵盖：人才培养靶场和线上线下培训平台及相关视频、实验、场景和考核内容；涵盖 web 安全、渗透测试技术、通信安全、物联网安全、安全防御方案及设备、加密解密技术等多种方向课程体系。	软 硬 件 一 体 化
2	赛场	根据科技馆作为强网杯永久赛场的需求以及平时作为其他多种类型竞赛场地的诉求，除舞台、屏幕、桌椅等基础设施外，在原有靶场功能上，定制烽火台反作弊监控平台展示装置、比赛全过程管理后台展示装置和攻防脚本推演系统等系统模块。同时利用场地的地形优势，设计了靶场秀模块，利用室内定位系统与靶场系统进行交互，让参观者能够简单的置身靶场其中。	软 硬 件 一 体 化
3	数字化展陈	为打造一个交流、展示、学习的平台，在网安馆共部署 24 台触控一体机，搭载保密教育微电影、网安动漫大点播、安全知识加油站等软件系统；意识闯关、安全射击、安全挑战、守护安全、保卫网络、技能比武、安全逃脱等测试系统；密码安全度测试、密码泄露检测站、安全感测试、CTF 初体验四项竞技体验系统。	软 硬 件 一 体 化
4	网络教室-网安馆专用人才培养靶场	根据不同群体和安全角色打造一间网络教室，布置桌椅、电脑、大屏幕等基础硬件设施外，部署 10 大网络安全竞赛系统：网络安全竞赛 CTF 个人赛平台、网络安全竞赛 CTF 团队赛平台、CTF 实训平台、网络安全众测平台、i 春秋信息安全在线教育平台、网络安全在线教育学习平台 PC 版、网络安全意识学习平台、网络安全竞赛培训平台、企业网络安全人才培养平台、网络安全人才在线培训认证系统。	软 硬 件 一 体 化
5	网络教室-攻防实战靶场	除桌椅、电脑、大屏等基础硬件设施外，搭建 web 自动化渗透测试系统、移动安全检测分析平台、Android 远控工具、GPU 本地密码破解平台、Linux 远控工具、U 盘打码器、Windows 远控工具、单兵工具箱等实战演练工具，支持学生动手操作，除培训功能外，也可作为攻防作战室。	软 硬 件 一 体 化
6	网络剧场	作为网安馆报告厅，除具备音响、灯光、舞台、大屏、幕布、座椅等基础设施外，搭配 15 分钟 3D 动画大电影，通过播放影片，以拟人化、故事化的手法，将智能手机的各种系统功能、应用 APP 和网络病毒拟人为一个个角色，建构了一个虚构的网络世界。通过现实世界的人物行为和虚拟网络世界中的人物、事件产生关联，来表现一场网络攻击事件的攻防全过程，从而对观众传播网络安全知识。	软 硬 件 一 体 化、 多 媒 体
7	守护网站安全	利用说明牌、图文设置、展台设置，并配置电脑主机、音箱等设备，部署一套安全状态展示系统软件，通过大屏幕进行展现。展示省行政区以及若干典型企业的网站安全状态，利用网络、数据、业务、应用、主机、环境等六个维度的数据全面分析和评估网站安全，向观众介绍保障网站安全需要关注的技术和方法，了解网站安全风险、短板的防御手段等，便于理解网站安全的预防策略和部署。	软 硬 件 一 体 化

序号	展项名称	交付内容	交付形态
8	等你来挑战	部署电脑桌和相关服务器和主机等设施，部署以公司赛事演练靶场为基础的软件平台，提供多种赛事模式和真题，使普通人也可以体验和了解安全竞赛的赛制、赛题、解题方式等，通过大屏幕进行展现夺旗赛体验赛、攻防赛体验赛、渗透赛体验赛三大赛制。	软 硬 件 一 体 化
9	万维之旅	设置镜头、激光雷达装置、投影、功放音箱等设备，部署互动系统软件，打造网络与我、虚拟与我、数据与我、无限与我、安全与我、现实与我 6 大场景，实现沉浸式互动体验。	软 硬 件 一 体 化
10	网络安全演练	设置可触控电视机、交换机、电脑主机、钢化玻璃等，部署演练软件平台，以游戏的形式将常规的安全演练过程制作作为普通观众容易理解的闯关答题模式，参观者通过简单的进行路径方向选项、行为动作选项等来完成闯关，通过播放相关图文和视频等了解演练内容，从而激发用户对于网络安全的兴趣、提升自我安全意识。	软 硬 件 一 体 化
11	我们·网络·世界-点阵空间智慧靶场	设置支撑架、LED 阵列、路由器、无线装置、主机、工控机等设施，并部署靶场软件平台，利用了数字化仿真方式以及靶场展示引擎的空间转换算法及模式，对每个分块屏幕上的显示数据和内容以及空间位置、展现角度等进行统一的控制和调度，通过 266 块大屏幕，展现赛博空间的科技感和创新思维，激发灵感和对网络安全的思考。 得益于靶场对场景中节点的数据采集、软件定义网络、控制数据投放、场景自检及重置等优势，提升展品的控制能力和容错能力，并可将点阵的初始形态制作成多种场景模板在数据库中长期留存，快速切换，并支持多任务并行管理能力，具备较好的扩展性和兼容性。	软 硬 件 一 体 化、 多 媒 体
12	时空长廊-体态互动智慧靶场	部署大型 LED 屏、高性能主机、交换机等设施和公司靶场平台，使参观者可以通过物理移动、体态动作变化等与展品进行互动，将行为投射到赛博空间之中，改变和触发展品的变化，将网络安全知识、空间体态识别互动技术、场景构建与复现技术等多种技术相融合，在多维空间中使参观者沉浸式体验到网络赛博空间的时空变迁和无穷变化。 得益于靶场系统的高弹性和扩展能力，场景库中可存储多套不同的展示内容和既定场景组合方案，通过后台的配置进行定时切换、数量触发式切换等，动作识别库中也可设定复杂动作的模型进行精细化动作的快速识别和记录。靶场的任务后台数据管理能力使每种场景的交互动作数量、场景内容切换数量、交互人群数量等均可在后台进行查看、排序和数据统计分析，运维人员可查看最受欢迎的动作、场景内容等，指导后续的展示内容编排和升级。靶场平台的稳定性、易用性和扩展性对展品的运营和使用提供了良好支撑。	软 硬 件 一 体 化、 多 媒 体

三、网络安全科技馆项目收入归入网络靶场系列产品的依据

网络安全科技馆项目作为综合应用型网络靶场，是公司人才培养靶场、赛事演练靶场、智慧城市安全测试靶场和业务模拟仿真靶场的多场景综合性应用，按照靶场的应用场景来分类，网络安全科技馆项目中网络靶场系列产品的收入构成

如下：

单位：万元

靶场的应用场景	收入金额	占比
人才培养靶场	2,812.15	24.95%
赛事演练靶场	2,592.72	23.01%
智慧城市安全测试靶场	443.85	3.94%
业务模拟仿真靶场	74.90	0.66%
合计	5,923.62	52.56%

网络安全科技馆项目中网络靶场系列产品的收入包括人才培养靶场2,812.15万元、赛事演练靶场2,592.72万元、智慧城市安全测试靶场443.85万元以及业务模拟仿真靶场74.90万元，在项目总收入中占比分别为24.95%、23.01%、3.94%和0.66%。

（一）网络安全科技馆项目中人才培养靶场的应用

网络教室内直接部署了公司的人才培养靶场系统，涵盖靶场的春秋云管理系统，靶标库、场景库、工具库、教学库等多种内容资源，支持并发多任务的教学任务管理、班级管理、教学进度管理、人员自学管理等，支持对教学计划、课程体系、实验场景等进行全面的配置和新建，支持考试管理、自动或手动的考卷管理，支持知识内容与实验内容综合组卷等，可以秒级下发单人自学实验任务，也可以分钟级为百人以下班级统一下发实验资源或组织考试等，对教学过程、自学过程、人员的学习和考试的记录和过程等均可进行以班级为单位或以个人为单位的精细化管理。针对科技馆的科普属性和有针对性的行业教育属性，在此教室平台上，设置了为不同团体、单位和人群甚至包括小学生和社区人群的专有教学实验和课程体系，能够支撑科技馆的各种日常的安全意识或专业技能实训需求。本教室主要面对科技馆对外的云端线上教学能力，在平台中主要添加了链路管理、安全运维管理、资源高可用和一体化调度管理等系统和能力。同时也配置了更多的资源和并发承载能力，可支撑更大规模、更多任务的并发执行。

（二）网络安全科技馆项目中赛事演练靶场的应用

网络安全科技馆作为“强网杯”的永久赛场，公司部署了春秋云境赛事演练靶场，予以长期平台支持。该平台支持CTF、AWDP、靶场赛、RHG等几乎所有的主流竞赛模式，拥有工具库、靶标场景库、历年赛题真题库等资源，支持对

赛前、赛中和赛后的各项精细化管理，能够支持数十人至数百人并发的各类网络安全赛事。

网络安全赛事通常对参赛人员的攻防技能有一定的要求，为了能够使普通人也可以体验和了解安全竞赛的赛制、赛题、解题方式等，基于春秋云阵靶场的赛事演练靶场，“等你来挑战”展项选取历次安全大赛中经典的入门和高级赛题，制作了此产品，形象化的让普通人员也能体验参赛选手的参赛过程和解题方法。

（三）网络安全科技馆项目中智慧城市安全测试靶场的应用

基于公司智慧城市安全测试靶场，“我们·网络·世界-点阵空间智慧靶场”展项利用靶场基础平台的虚实结合设备管控系统，设置两百余个管控电机的网络拓扑场景，在场景中设置节点控制系统，利用点阵管理的方式完成对场景中数百个电机的控制。得益于靶场对场景中节点的数据采集、软件定义网络、控制数据投放、场景自检及重置等优势，提升展品的控制能力和容错能力，并可将点阵的初始形态制作成多种场景模板在数据库中长期留存，快速切换，并支持多任务并行管理能力，具备较好的扩展性和兼容性。

基于公司智慧城市安全测试靶场，“时空长廊-体态互动智慧靶场”展项使用公司的场景管理后台模块进行场景和展示效果的统一管理和控制，利用动作行为采集系统实现与场景的交互管控，定制体态识别、容错模块提升识别效率和效果，数字化特效模块完成展示内容的衔接控制。得益于靶场系统的高弹性和扩展能力，场景库中可存储多套不同的展示内容和既定场景组合方案，通过后台的配置进行定时切换、数量触发式切换等，动作识别库中也可设定复杂动作的模型进行精细化动作的快速识别和记录。靶场的任务后台数据管理能力使每种场景的交互动作数量、场景内容切换数量、交互人群数量等均可在后台进行查看、排序和数据统计分析，运维人员可查看最受欢迎的动作、场景内容等，指导后续的展示内容编排和升级。靶场平台的稳定性、易用性和扩展性对展品的运营和使用提供了良好支撑。

（四）网络安全科技馆建设项目中业务模拟仿真靶场的应用

基于公司业务模拟仿真靶场，“我的包裹安全吗？”展项模拟城市快递储物箱使用场景，使用了靶场的场景构建系统来设计和规划了快递储物箱多个电子操作模块之间的数据传递框架和认证流程，并在场景框架构建起来后，定制开发了

快递储物箱内部的多个仿真业务模块，包括快递储物箱操作流程、用户管理和密码认证逻辑、数据存储过程，机械反馈原理等，高逼真的复现了快递储物箱业务模拟场景的典型流程以及在此流程中可能出现的多个安全脆弱点环节。利用公司靶场的场景下发、重置、自测等流程对场景及场景中模拟的业务系统模块进行统一管理，保障场景的稳定性和高可用性。在后续场景升级或改造等过程中，由于应用了靶场的相关技术和模块，也使得场景调整成本大大降低。

四、公司对该类业务的规划，是否会持续发生

网络安全科技馆是公司网络靶场系列产品中综合应用型网络靶场的典型应用，该类业务是公司网络安全产品中的重要组成部分。该类业务是公司在经历320余场不同业务场景的网络靶场构建，超过38万人次的网络靶场运行数据积累，百万级中低交互集群城市级网络靶场搭建，并为十余个行业提供网络靶场产品与服务之后，方取得的业务机会，是公司长期技术积累和市场品牌影响力的结果。

随着国家网络空间安全战略的实施、《网络安全法》《数据安全法》以及《关键信息基础设施安全保护条例》的颁布实施，国家、政企及个人网络安全需求不断提升，以网络安全科技馆为代表的综合应用型网络靶场将迎来更大的市场机会。该类业务是公司未来发展战略规划中必要的产品组成部分。公司在组织架构、研发、市场开拓等方面对该类业务进行了规划和部署。

1、专门成立数字创意事业部来负责该类业务的开展，数字创意事业部的具体组织架构如下：

序号	部门名称	部门职责
1	数字创意事业部-销售部	负责为公司开拓网络安全科普教育及综合应用型网络靶场建设方面业务
2	数字创意事业部-产品研发部	负责公司展览展陈类产品研发以及项目支撑等相关工作

2、公司针对类似业务专门进行了产品研发，包括网络安全意识和科技体验教育平台和行走的网安馆产品等在研项目，具体如下：

序号	研发项目名称	研发子项目	所处阶段	预计达到的目标	研发项目及成果技术水平
1	网络安全意识和科技体验平	网络安全人才培养基地方案设计策划、项目运营建设	产品设计及推广阶	实现网络安全科技馆类产品整体解决方案推广，策划、研发和制作网络安全意识、技能知	基于实际案例，通过整合公司在各行业的经验积累，综合进行策划设计，提高广大群众网络

	台	网络反诈知识体系及展陈展品策划设计 网络安全科普漫画出版	段	识等的活动、展陈品以及配套物料等。	安全意识及防范新型诈骗能力素养。
2	行走的网安馆产品	AI 换脸 照片背后的秘密 2.0 密码强度对抗台 声临其境 窃密与反窃密 蜜罐及智能家居等	产品研发	将科技馆展品小型化、移动化，配置到可以移动搬运、快速搭建和就地安装的各类展陈设备，对原有重点展品进行二次开发或重新制作，达到移动展陈的产品目标。	通过前沿智能科技，让用户体验智能时代技术先进性的同时，认知到网络风险性的一面，在后续生活工作中提升网络安全风险防范意识。
3	保密安全意识靶场	普通大众保密安全意识科普体系 专业保密安全知识体系	产品研发	以保密知识体系为主线，重点通过保密工作中“管理+技术+文化”三大领域，体系化、全面化科普保密知识。	采用大数据、人工智能等新兴科技，拟打造网络攻防对抗靶场、AR/VR 知识学习区、网络安全态势感知、大数据情报分析体验、网络安全攻防实训比赛等产品，打造高科技水平保密安全意识靶场。

3、跟进其他地方的科技馆项目

随着网络安全科技馆的顺利运营，公司在网络安全展馆类业务积累了较好的经验和竞争优势，目前已顺利在广东省、福建省以及河南省签订类似项目，各项目详情如下：

单位：万元

序号	客户名称	项目名称	合同金额
1	三明市发展和改革委员会	数字中国建设峰会论坛和展览服务	193.00
2	郑州天健网安技术有限公司	行走的网络安全科技馆展项系统开发一期	75.00
3	郑州天健网安技术有限公司	行走的网络安全科技馆展项系统开发二期	75.00
4	广发银行股份有限公司	广发银行庆祝建党 100 周年网络安全专题技术支撑服务	61.50
5	广州市公安局	网络安全 110 宣传日-网络安全科普体验展	28.50
6	中共北京市委网络安全和信息化委员会办公室	2021 年网络安全宣传周活动经费--网络安全技能宣传活动组织	74.45
7	三明市水利局	第四届数字中国建设成果展览会上提供展示内容的设计和技术支撑工作	3.10
	合计		510.55

此外，其余省市也在积极筹划各具特色的类似项目。该类业务的后续业务形态包括展馆类项目和会务会展。展馆类项目包括馆内主题展、行业馆和移动馆等，会务会展包括行业展会、发布会前展览、主题临展和定制展览等。后续商机项目的详情如下：

业务形态	商机项目	区域
展馆类项目	2022 国家网络安全宣传周—合肥	安徽
	河南周口分馆	河南
	反诈主题场馆	广东
	熊猫馆（网安主题科技馆）	广东
	保密意识教育馆建设	广东
	取证博物馆二期	江苏
	三明红谷会客厅	福建
会务会展	淮北市青少年网安科普展厅	安徽
	密云科技馆	北京
	网络安全 110 科学城展览	广东

4、网络安全科技馆的后续运营收入

随着网络安全科技馆的顺利运营，公司已经和天健网安签订相关后续合同。基于网络安全科技馆深入基层的需求，研发出移动式、小型化、全封装的网络安全科普宣教平台（网络安全大篷车），解决了网络安全意识普及性教育问题。

另外，公司正在跟进网络安全科技馆后续运营过程中的商机项目。首先是在网络安全科技馆的运营过程中，会根据专家组的意见，对展品展项进行不断提升改造，申请增加新的项目内容；其次，第五届“强网杯”将在网络安全科技馆举办一系列的延伸活动，包括网络安全先进技术成果展、强网初心红色记忆展、强网科普展等。公司正在跟进潜在的商机项目，这些项目有可能带来新的收入增长。

综上所述，网络安全科技馆项目是公司未来发展战略规划中必要的产品组成部分。虽然全国性单体大规模的科技馆类项目在短期内可持续发生尚存在不确定性，但公司已在组织架构、研发、市场开拓等方面对该类业务进行了规划和部署，密切跟踪市场中的商机项目，并且已签订了部分项目合同。

（2）结合报告期内网络靶场与人才培养业务单个项目收入较低、网络安全科技馆建设项目具有偶发性的特点，以及目前在手订单情况等，说明公司业绩的

可持续性，发行人是否持续符合上市标准；

一、网络靶场与人才培养业务的单个项目收入

报告期内，发行人网络靶场系列产品、线上线下培训的单个项目收入如下：

单位：万元

分类	2021 年 1-6 月			2020 年		
	项目数量	收入	单个项目收入	项目数量	收入	单个项目收入
网络靶场系列产品	34	4,825.01	141.91	63	18,069.30	286.81
线上线下培训	31	323.33	10.43	111	945.44	8.52

(续上表)

分类	2019 年			2018 年		
	项目数量	收入	单个项目收入	项目数量	收入	单个项目收入
网络靶场系列产品	81	6,339.87	78.27	114	9,954.01	87.32
线上线下培训	94	1,061.87	11.30	118	973.59	8.25

公司网络靶场系列产品的收入稳步提升，从 2018 年的 9,954.01 万元增长到 2020 年的 18,069.30 万元。2021 年 1-6 月公司网络靶场系列产品受季节性影响，上半年收入较小，但是单个项目收入金额较 2018 年和 2019 年明显提高。2020 年单个项目收入较高，主要受网络安全科技馆项目的影响，剔除网络安全科技馆单一大型项目收入影响，2021 年 1-6 月单个项目收入高于 2020 年度，公司执行大项目的能力增强。公司网络靶场系列产品具有先发优势，在各个行业具有广阔的市场机会，随着公司项目经验不断丰富，公司员工数量从 2020 年末的 343 人上升到 2021 年 6 月 30 日的 394 人，增加 14.87%。总体而言，公司具有技术、人员、项目经验以及经营需要的资金，公司上市后募投项目的实施将继续增加公司业绩的可持续性。

1、网络靶场系列产品项目的平均收入呈上升趋势

公司网络靶场系列产品早期主要应用在人才培养和赛事演练，随着技术进步和客户需求推动，网络靶场系列产品衍生出不同的应用场景，具备了更多软件功能模块、配套服务和增值服务，解决的问题越发广泛，网络靶场价值不断提升。报告期内，网络靶场系列产品的单个项目平均收入由 87.32 万元增长到 2020 年的 286.81 万元，2021 年单个项目平均收入为 141.91 万元。剔除网络安全科技馆

项目后，报告期内，网络靶场系列产品的单个项目平均收入由 87.32 万元增长到 141.91 万元，网络靶场系列产品项目的平均收入呈上升趋势。

2、公司网络靶场系列产品在行业市场中具有先发优势

公司早期主要向公安以及其他政府部门销售靶场产品。公司中标的公安部和一些省公安厅的靶场项目成为行业“样本工程”，起到示范效应。随着公安体系网络靶场建设的不断推动，省、市各级单位陆续开展靶场建设。公司已经在上述领域进行了深入的市场开拓，具有明显的先发优势，形成了一定的市场壁垒。

3、网络靶场系列产品在多个行业具有广阔市场机会

通过 320 多场赛事演练活动积累的数百个行业级场景，近百个城市级仿真互联网场景和在公安行业积累的网络靶场项目经验，公司网络靶场系列产品已覆盖教育、通信、交通、国防工业、能源、金融、政法、电子政务、科技、互联网等十余个重点行业，伴随着重点行业对网络安全需求的不断提升，公司将获取更多的业务机会。公司靶场的主要应用场景和在手订单情况如下：

序号	应用场景	已完成项目	在手订单情况	在手订单未确认收入金额（万元）
1	赛事演练靶场	强网杯、纵横杯、巅峰极客、护网杯、网鼎杯等	中国电信集团-浙江培训基地建设项目等	32.57
2	人才培养靶场	紫金山实验室、哈尔滨工业大学等人才培养的靶场建设和服务项目	南方电网科研院融合靶场项目	1,296.36
3	智慧城市安全测试靶场	广东省政务服务数据管理局 2019 年网络安全体系之靶场及演练培训服务项目、2018 年广东“数字政府”政务信息化安全服务采购项目、2019 年网络安全体系之深度测试服务项目	中铁信攻防平台建设项目、基于网络数据处理技术-评估调度子系统项目等	736.35
4	案件线索追踪实战靶场	南京市公安局、广州市公安局、山西省公安厅等案件线索追踪实战靶场建设和服务项目	南京市公安局网络安全实验室二期项目、网络靶场（内外网双靶场联动）项目等	4,524.68
5	业务模拟仿真靶场	国网新源控股有限公司检修分公司、国网湖南省电力有限公司、广州供电局、国网宁夏电力有限公司、华润电力等业务模拟仿真靶场建设和服务项目	中国人民解放军靶场培训平台项目等	1,480.02

6	人工智能攻防靶场	全球能源互联网研究院有限公司、北京一三一八单位、国家计算机网络与信息安全管理中心、海南社会经济发展研究中心等人工智能攻防靶场建设和服务项目	暂无相关在手订单	-
7	复杂业务安全推演靶场	浙江大学、中国信息安全测评中心、中海油信息科技有限公司、石化盈科信息技术有限责任公司、平安银行股份有限公司等复杂业务安全推演靶场建设和服务项目	浙江大学物联网安全检测和实时监测体系与方法研究项目等	330.19
合计				8,400.17

二、网络安全科技馆项目的偶发性

（一）公司运作大项目的能力增强，在手订单中大项目数量明显上升

公司专门成立了数字创意事业部、战略拓展部、特种行业技术委员会及解决方案中心，以解决大项目的开拓、实施、交付等重要环节。同时，随着公司承接网络安全科技馆项目、基于网络数据处理技术项目、广东省“数字政府”网络安全深度测试服务项目等一系列大项目的实施和交付，公司运营大项目的经验和能力显著提升。

随着公司技术的积累和运营能力的提升，公司获取大项目的能力不断增强，获取的大项目数量不断增加。截至 2021 年 11 月 30 日，公司金额较大的合同数量明显增加。500 万以上的合同数量为 15 个，较上年同期增加 6 个；1,000 万以上的合同数量为 5 个，较上年同期增加 1 个。大项目数量的增加，削弱了单一项目对公司业绩的影响。

（二）综合应用型网络靶场的市场需求不断增加

随着国家网络空间安全战略的实施、《网络安全法》《数据安全法》以及《关键信息基础设施安全保护条例》的颁布实施，国家、政企及个人网络安全需求不断提升，以网络安全科技馆为代表的综合应用型网络靶场将迎来更大的市场机会。

（三）依托科技馆的技术积淀，网络安全展馆类项目增多

随着网络安全科技馆的顺利运营，公司在网络安全展馆类业务积累了较好的经验和竞争优势，目前已顺利在广东省、福建省以及河南省签订类似项目。并且，公司正在持续跟进北京、安徽、广东等其他省市的类似业务商业机会。

随着网络安全科技馆的顺利运营，公司已经和天健网安签订相关后续合同。

另外，公司正在跟进网络安全科技馆后续运营过程中的商机项目，包括原有展品展项的提升改造和新展品展项的增加、第五届“强网杯”青少赛系列延伸活动等。

三、在手订单

（一）在手订单概况

截至 2021 年 11 月 30 日，公司正在履行的合同金额为 22,854.61 万元，合同数量为 115 个，具体情况如下：

单位：万元

合同金额区间	2021 年 11 月 30 日		2020 年 11 月 30 日	
	合同数量	合同金额	合同数量	合同金额
大于 1,000 万	5	7,543.24	4	17,011.74
500 万-1,000 万	10	6,729.52	5	3,343.66
100 万-500 万	28	6,327.57	36	8,517.20
50 万-100 万	16	1,218.48	30	2,097.28
10 万-50 万	33	939.57	53	1,464.17
小于 10 万	23	96.22	44	206.40
合计	115	22,854.61	172	32,640.45

截至 2021 年 11 月 30 日，公司金额较大的合同数量明显增加。500 万以上的合同数量为 15 个，较上年同期增加 6 个；1,000 万以上的合同数量为 5 个，较上年同期增加 1 个。大项目数量的增加，削弱了单一项目对公司业绩的影响。截至 2021 年 11 月 30 日，在手订单合计金额较 2020 年 11 月 30 日下降，主要受 2020 年单一大型项目影响。剔除单一大型项目网络安全科技馆的影响，2021 年 11 月 30 日公司在手订单与公司 2020 年 11 月 30 日持平。

按照产品与服务类别划分，公司正在履行的合同情况如下：

单位：万元

分类	合同金额（含税）	占比
网络安全产品	16,969.32	74.25%
其中：网络靶场系列产品	13,810.61	60.43%
安全管控与蜜罐产品	1,911.80	8.37%
安全工具类产品	1,246.91	5.46%
网络安全服务	5,885.29	25.75%
其中：安全防护系列服务	4,715.25	20.63%

网络安全竞赛服务	542.17	2.37%
其他服务	627.87	2.75%
合计	22,854.61	100%

2021年11月30日公司的在手订单主要集中在网络安全产品，合同金额为16,969.32万元，占比为74.25%，包括网络靶场系列产品13,810.61万元，安全管控与蜜罐产品1,911.80万元，以及安全工具类产品1,246.91万元。此外网络安全服务的合同金额为5,885.29万元，占比为25.75%。

公司正在履行的500万元以上主要合同的信息如下：

单位：万元

序号	客户名称	合同内容	合同金额	签署年份	合同状态
1	昆山九华电子设备厂	基于网络数据处理技术-评估调度子系统	2,486.96	2020年	正在履行
2	南京市公安局	网络安全实验室二期	1,466.00	2021年	正在履行
3	广东省公安厅	广东省公安网络靶场	1,280.00	2020年	正在履行
4	中国科学院信息工程研究所	网络系统及使用环境建设	1,253.00	2020年	正在履行
5	河池市公安局	河池市公安局网络建设项目（一期）	1,057.28	2020年	正在履行
6	北京市对外服务办公室	安全防护服务项目	837.00	2020年	正在履行
7	广东省政务服务数据管理局	广东省“数字政府”网络安全深度测试服务项目（2020年）	833.36	2020年	正在履行
8	中国人民解放军	靶场培训平台项目	825.14	2021年	正在履行
9	南京景枫教育投资管理有限公司	青少年信息安全教育实训靶场开发	679.32	2021年	正在履行
10	南方电网科学研究院有限责任公司	网络安全靶场平台及能力建设项目	675.00	2020年	正在履行
11	神州网云（北京）信息技术有限公司	网络探针采购及技术开发服务合同	621.30	2021年	正在履行
12	泰安市公安局	网络靶场系统采购项目	592.00	2019年	正在履行
13	中国人民解放军	春秋云境网络靶场项目	589.50	2021年	正在履行
14	广东省政务服务数据管理局	省数字政府常态化网络安全演练与培训服务（2021年）项目	568.60	2021年	正在履行

（二）在手订单进度

公司在手订单的合同总金额为22,854.61万元，其中6,755.25万元已确认收

入，16,099.36 万元未确认收入，具体情况如下：

单位：万元

合同金额区间	合同金额 A	已确认收入部分 (含税)		未确认收入部分 (含税)	
		金额 B	占比 C=B/A	金额 D	占比 E=D/A
大于 1,000 万	7,543.24	2,981.10	39.52%	4,562.14	60.48%
500 万-1,000 万	6,729.52	1,753.72	26.06%	4,975.80	73.94%
100 万-500 万	6,327.57	1,498.37	23.68%	4,829.21	76.32%
50 万-100 万	1,218.48	312.53	25.65%	905.95	74.35%
10 万-50 万	939.57	178.84	19.03%	760.73	80.97%
小于 10 万	96.22	30.70	31.91%	65.52	68.09%
合计	22,854.61	6,755.25	29.56%	16,099.36	70.44%

注：已确认收入部分系一个合同中约定了若干单项履约义务，部分履约义务已执行或者执行完毕，按照既定的收入确认原则已确认相应收入。

(三) 2021 年预计全年合同签订及执行情况

公司 2021 年预计全年合同签订及执行情况如下：

单位：万元

分类	金额
截至 11 月 30 日已确认收入（不含税）	20,226.48
截至 11 月 30 日在手订单（含税）	22,854.61
12 月预计签单项目（含税）	13,912.23

截至 2021 年 11 月底，发行人在手订单金额达到 22,854.61 万元，其中 16,099.36 万元未确认收入，在手订单较为充裕，业务拓展情况良好，业务开展的可持续性较好。

综合来看，网络靶场业务仍处于起步阶段，根据客户需求，可叠加不同的功能模块和应用系统，单个项目收入的增长潜力较大。尽管网络安全科技馆建设项目具有偶发性，公司的在手订单充裕，业务扩展情况良好，公司业绩具有可持续性，发行人持续符合上市标准。

(3) 网络安全科技馆建设项目的合同主要内容与招投标是否一致，收入金额调整的原因、过程、与工作量的匹配关系，项目验收时点、内容与合同约定的一致性；

一、合同主要内容与招投标是否一致

（一）合同主要内容与招投标是否一致

从工作内容、项目内容、合同工期、质量标准、合同价款等方面来看，网络安全科技馆项目的合同主要内容与招投标基本保持一致，具体条款对比如下：

招标文件条款		合同条款		是否一致
一、招标范围及服务要求		2.项目工作内容		
(一) 招标内容范围		2.1.乙方工作内容		
1.1 方案设计	依据展陈大纲并结合现场实际，负责开展项制作及布展施工进行详细设计，直至完成满足施工所需的全部施工图设计（施工图包含现场土建改造、布展环境装饰、展品展项制作、导览导视、配套强弱电系统及展览智能化控制系统）。	2.1.2.展示初步设计	整个展厅及展区的详细平面图、立面图、鸟瞰图及环境形式设计图、展厅虚拟漫游视频（不少于 5 分钟）。	一致
1.2 展项制作	依据详细设计方案，负责全部展品、展项及设备的采购、制作、安装和系统集成。另须配合招标人完成对展品展项的调研、询价与确认。	2.1.1.信息安全展示软硬件展品设计及研发	信息安全展示硬件部分包括采购的高科技展品、展项、硬件设备、网络设备及相应维护设备。	一致
			信息安全展示软件设计研发包括开发高科技数字化展陈系统及组件、固化的软件产品、第三方软件产品或中间件、按甲方需求定义设计和（或）二次开发、实施、配置的数字化展陈系统等。	一致
1.3 布展施工	依据详细设计方案，负责对现场土建及原有安装按需改造或调整（原有附属物或安装物投标人在满足设计、规范及安全的情况下自行按需拆除或利用），负责布展环境装饰施工及全部配套安装（含强电系统、弱电及展览智能化控制系统展厅内部安防监控配合系统的安装等展览所必备的功能设施）。	2.1.6.布展设计及施工（但不限于）	展厅、展区、展品总体平面布置设计及施工；	一致
			展厅、展区环境设计（地面、墙面、顶部、隔板、隔墙、背景墙、场景、造型等）及施工；	一致
			针对展品特殊要求的环境、安装基础和供配电基础设计及施工；	一致
			展品的水、电、气、网络等外部接口综合布管布线的基础设计及施工。	一致
		2.1.7.相关配套服务工作	负责信息安全展示软硬件展品设计及研发、展品制作（含购置）、系统安装及调试、数字化解决方案、土建总包等工作的总体协调及分包单位的协调。	一致
1.4 布展运营配合服务		2.项目工作内容 4.质量标准		
1.4.1	项目验收后两年内，投标人须在	2.1.4.系	系统安装及调试包括展品安	一致

	招标人要求的时限内无偿提供以下服务：展项、设备、基础装饰等硬件的维护、维修；展板文字、多媒体内容等软件的更换和更新；在招标人明确提出以上服务后，投标人须在 4 小时内现场响应，并在投标文件中响应售后方案。	统安装及调试	装调试、试运行，直至通过验收；对甲方的操作人员及维修人员进行技术培训。	
1.4.2	提供系统操作指南并对招标人管理团队和解说员进行操作培训。	4.1.2.软硬件产品研发质量保证	乙方在合同约定的质保期内向甲方提供免费的保修和维护服务。在此期间如发生系统运作故障，或出现瑕疵与缺陷，乙方将按照下列方式提供保修和维护服务：系统普通故障、个别服务不正常，48 小时内答复，7 个工作日内恢复正常工作；系统严重故障、部分服务不正常，10 个工作日内答复，30 个工作日内恢复正常工作；	一致
(二) 实施进度要求		3.合同工期要求		
2.1	招标人签发正式开工令后 200 个日历日内完成所有展项的设计、采购、制作、布展与施工	3.1.乙方项目总体进度	进场准备日为 2020/4/20，项目完工日为 2020/8/10，共 113 日历天。	一致
二、人员要求		4.质量标准		
2.1	投标人一旦中标，项目负责人在整个项目实施期内必须在位。项目负责人未经招标人书面同意，中标人不得更换，否则招标人有权终止合同。	4.4.项目管理及质量标准	乙方在投标文件中承诺的设计负责人、设计班子主要成员、项目经理及相应资质的专业技术、管理人员未经甲方书面同意，不得调换或撤离，并按工程进度及时到位。	一致
2.2	中标人未能按照承诺到岗尽职的，招标人将视情况严重程度对其作出相应处理，给予警告并发出整改通知。	4.4.项目管理及质量标准	如项目经理及相应资质的专业技术人员未按照要求到位，经甲方书面催告后乙方仍拒绝改正的，视作违约，甲方有权单方面终止合同；	一致
			项目经理及其他管理人员到位率都应在 90%以上。	一致
三、投标报价		6.合同价款		
3.1	本项目为信息系统集成化一体化招标，投标人采用总价包干方式。投标人投标报价不得超过招标控制价 1.87645 亿	6.1.合同中标价	本合同中标价为：（大写）壹亿捌仟柒佰伍拾万元整，（小写）187,500,000 元。	一致

(二) 合同约定的主要展项与招投标是否一致

在展馆建设的过程中，公司根据业主和专家组的意见对展项做出调整。和招投标文件相比，合同约定的展项存在约 20% 的差异。具体来看，新增展项 10 余

件，主要包括网场点兵、黑客密室、赛事风云等；删除 30 余件展项，分别为：走进智能家居、网站的构造、网站安全拼图版等。调整展项 60 余件，主要是名称调整、内容优化等，使得展项的设计和呈现更符合场馆定位，观众体验更佳，并不涉及对展项的实质性调整。在展陈行业，实际建造中的展项细节调整属于常见现象。

二、收入金额调整的原因、过程、与工作量的匹配关系

（一）投标文件中关于联合体成员工作量的预估比例

公司与合肥探奥作为联合体投标单位，在投标过程中对相关的服务范围进行了约定，“联合体各成员单位内部的职责分工如下：永信至诚负责科技馆项目的信息安全展示软硬件展品设计及研发、系统安装及调试、数字化解决方案、展品制作（含购置）、场馆智慧化等全部工作；合肥探奥负责科技馆项目的展馆初步设计、展示环境深化设计及布展、室内装饰装修工程、展馆内部施工等工作。按照本条上述分工，联合体成员单位各自所承担的合同工作量比例如下：75%：25%。”因此公司和合肥探奥在投标阶段对双方将会产生的工作量进行粗略的预估，并不代表最终的收入结算比例。此外，投标文件中也明确规定“投标工作和联合体在中标后项目实施过程中的有关费用按各自承担的工作量分摊”。

（二）收入金额调整的原因、过程、与工作量的匹配关系

在科技馆项目中，公司主要负责软硬件展品的开发与研发、系统安装及调试、数字化解决方案、多媒体展示，以及对项目整体的设计和管理。合肥探奥主要负责准备材料来完成室内的装饰装修工程、展馆内部施工，以及准备部分展项的硬件设备。根据每一个展项中所实际承担的工作内容，来进行各个展项收入金额的分摊。各主要展项中公司和合肥探奥分别承担的工作内容，以及根据工作内容所分配的收入金额如下：

单位：万元 序号	展项名称	公司承担的工作内容	公司分摊的金额（含税）	合肥探奥承担的工作内容	合肥探奥分摊的金额（含税）
1	赛场	1、完成靶场秀互动定制游戏系统的开发和研制，包括以下分系统： （1）综合管理分系统，可分为用户管理子系统和角色管理子系统。 （2）网络安全攻防业务管理系统，可分为事件记	1,347.33	1、提供舞台灯光、舞台扩声、舞台机械等设备。 2、搭建移动式舞	839.18

单位：万元 序号	展项名称	公司承担的工作内容	公司分摊的金额（含税）	合肥探奥承担的工作内容	合肥探奥分摊的金额（含税）
		录子系统和事件应用子系统。 （3）攻防态势感知系统，可分为攻防态势感知系统和防御态势感知子系统。 （4）攻防事件管理分系统，可分为主屏显示子系统、辅助屏展示子系统、环形屏展示子系统。 （5）网络远程管理系统，可分为网络安全应急响应平台和网络远程管理系统。 （6）软件资源包，包括郑州市虚拟 3D 模型包和场景包。 2、完成靶场秀中营造 16 个场景的多媒体制作工作。		台、屏体升降系统，以及悬挂支架。 3、提供阻燃板、网线、方管等材料。	
2	网络教室-网络安全在线云靶场	提供 e 春秋网络安全实验室靶场系统，包括虚拟仿真分系统、比武竞赛分系统、安全实训分系统、综合管理分系统、软件资源包以及精品课程定制	1,473.84	1、提供 LED 屏等设备。 2、提供方管等材料，安装骨架，进行焊接、打磨和防锈处理。	10.83
3	数字化展陈	1、提供网安动漫大点播，包括 12 节视频动画的前期动漫脚本策划、场景细化、动漫设计、配音、动漫剪辑和制作工作。 2、提供安全知识加油站软件，包括 400 节视频资源，可以平滑展示网络安全科普的全部视频。 3、保密教育微电影，包含 15 节视频资源的剧本策划、视频拍摄、剪辑、制作、视频播放系统和视频展示系统。 4、提供密码安全度测试和密码泄露检测站，体现出动态交互效果及动画设计，增加游戏趣味性与交互性。 5、提供安全感测试，结合生活、工作场景进行模拟人物场景设定，制定脚本，按照脚本进行 20 张场景及角色手绘图片设计。根据题目描述，设计题目场景，进行安全感测试。 6、提供 CTF 初体验，CTF 在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。 7、提供 160 道安全防护知识题目，通过投篮游戏展示答题效果。 8、提供 120 道网络发展成就、发展历程及人才培养的题目，通过寻宝的方式展示游戏效果。 9、提供 500 道安全防护知识题目，答题完成后显示星级、得分、提示信息。 10、提供 200 道安全事件及行为判断的题目整理，通过判断题的方式进行答题并实时计算结果。	1,164.63	1、对展台和座椅进行加工。 2、提供方管、板材、油漆等材料。	15.86

单位：万元 序号	展项名称	公司承担的工作内容	公司分摊的金额（含税）	合肥探奥承担的工作内容	合肥探奥分摊的金额（含税）
		11、提供 200 道网络安全法、等级保护法等网络安全相关法规题目，支持通过九宫格来展示游戏效果。			
4	网络教室-网安馆专用人才培养靶场	1、完成网络安全竞赛 CTF 个人赛平台、网络安全竞赛 CTF 团队赛平台、CTF 实训平台、网络安全众测平台、i 春秋信息安全在线教育平台、网络安全在线教育学习平台 PC 版、网络安全意识学习平台、网络安全竞赛培训平台、企业网络安全人才培养平台、网络安全人才在线培训认证系统等 10 项软件产品的开发和研制。 2、提供的软件产品包括架构设计、定制开发、账号系统、展示系统、答题系统等模块。 3、提供台式机、服务器等设备。	1,012.16	1、提供 LED 屏等设备。 2、提供方管等材料，安装骨架，进行焊接、打磨以及防锈处理。	21.79
5	网络剧场	提供 15 分钟的影院级三维动画片，重点用于展示网络安全的重要性。3D 影院级动画的制作包括剧本创作、3D 角色设计、场景设计、导演执导、分镜头制作、动画渲染、流体碰撞线条等复杂特效、原创音乐、音效合成、剪辑输出等环节。	429.40	提供剧场灯光、音响系统、投影机镜头、影院融合系统等设备。	465.09
6	我们网络世界-点阵空间智慧靶场	1、提供动屏可视化系统，软件开发包含电机控制通讯系统、电机运动控制系统、图形设计模块、图形处理系统、屏幕显示通讯模块等多个子系统，覆盖屏幕运动、显示、后台管理等多个系统模块。 2、提供定制多媒体，提供包括 3D 场景结合流体、碰撞、线条等复杂特效，包括剧本创作、导演执导、场景设计、特效制作、分镜头制作及动画渲染、音效合成、输出等 3D 动画的制作。	235.61	1、提供减速机、显示屏体等设备。 2、提供钢板、方管等材料。 3、完成激光切割，钻床打孔焊接打磨、电器柜控制电路、制作等工作。	512.55
7	网络教室-攻防实战靶场	1、完成 Web 漏洞挖掘系统软件的开发和研制，具备完善的任务管理功能。 2、提供安卓安全检测系统，对样本进行基础信息扫描与探测，抓取样本商店上线名称、图标运行版本等样本的标识性信息， 3、提供安卓木马样本主动获取与综合分析系统，可通过控制端界面查看目标安卓手机的文件列表，支持对该列表中的文件和目录进行下载、删除操作，同时可通过添加文件功能，将指定文件上传至目标手机中。 4、提供泰坦 GPU 高速计算平台，支持多种类型的加密数据， 5、提供 linux 安全检查工具软件，可通过控制端界面查看目标 Linux 系统的文件列表，直观展示文件名称、文件大小、修改日期和权限等信息，支持对该列表中的文件和目录进行新增、删除等操作，同	613.46	1、提供 LED 屏等设备。 2、提供方管等材料，安装骨架，进行焊接、打磨以及防锈处理。	10.83

单位：万元 序号	展项名称	公司承担的工作内容	公司分摊的金额（含税）	合肥探奥承担的工作内容	合肥探奥分摊的金额（含税）
		时可完成文件的上传和下载，确保传输文件的完整性。 6、提供终端及互联网行为监测系统，支持获取目标 Windows 系统的磁盘空间总大小以及剩余空间大小，能查看磁盘里面的详细内容，并且能针对目标文件进行增、删、改、查的基本功能，及文件上传和下载功能，支持断点续传功能。 7、提供网络安全单兵工具箱系统，内含不少于 200 款工具。 8、提供台式机、服务器等配套硬件。			
8	时空长廊-体态互动智慧靶场	1、定制化的多媒体，提供包括剧本创作、场景设计、分镜头制作、动画渲染等环节的 3D 动画制作。 2、提供体感互动系统，包括美术设计、体态识别模块等模块。 3、提供处理器、主板、显卡、体感摄像头等配套设备。	235.22	1、提供高清 LED 显示屏、电脑主机、五金以及电气辅材等设备。 2、提供方管等材料。	89.62
9	网络安全演练	以游戏的形式完成网络安全演练的定制开发，包括以下功能： 1、内置演练场景，支持为用户提供渗透演练的基础环境；采用闯关模式进行演练，通过划分不同的关卡体验不同的网络渗透方法和知识点。 2、用户管理，支持通过内置算法生成用户名称，并确保其唯一性，以此作为演练人员的登录账户，支持演练人员采用系统生成的用户名进行免密登录。 3、人机交互，支持基于图像的交互展示，在各场景关卡中使用图像提示渗透相关信息。 4、行为日志，日志采集和存储，针对用户的行为日志进行采集和记录，通过系统内置的日志数据处理机制实现对原始日志过滤、归并、存储，使其具备高可读性；日志查询和展示，能够针对记录的日志数据进行查询并以列表形式进行展示。 5、逻辑验证，支持将用户当前步骤与演练场景进行关联处理，以触发系统对演练步骤状态的评判机制。 6、演练排名，对于闯关成功的用户，系统将记录其应对关卡的成绩得分；系统会针对所有历史用户的闯关成绩从高到低进行排名。	242.95	1、提供脚本推演服务器、交换机、电脑主机等设备。 2、根据展项内容配图、绘制版面、确认字体展示效果，对电视机压板、电视机垫块等进行加工。	42.71
10	守护网站安全	1、展示省行政区以及若干典型企业的网站安全状态。 2、具体从网络、数据、业务、应用、主机、环境等六个维度全面分析和评估网站安全。 3、向观众介绍各个维度的监测技术。 4、通过评分模型，可以汇集问题数据进行加权计	259.90	1、提供拼接屏、高清处理器、触摸屏等设备。 2、进行激光切割、异形框架焊接等。	12.71

单位：万元 序号	展项名称	公司承担的工作内容	公司分摊的金额（含税）	合肥探奥承担的工作内容	合肥探奥分摊的金额（含税）
		算、得出分数，分数越高安全性越好。 5、通过数据趋势分析能够帮助评估网络安全风险、短板等，便于先导预防策略部署。			
11	等你来挑战	提供等你来挑战系列软件，包括以下分系统： 1、体验管理分系统，其中的竞赛体验中心子系统包括体验首页管理、体验赛规则管理等模块。 2、体验展示分系统，其中的体验赛可视化中心，包括轻量级夺旗赛界面、轻量级攻防赛界面等界面。 3、软件资源包，包括夺旗赛体验赛题包、攻防赛体验赛题包和渗透赛体验赛题包	249.21	提供电脑桌、显示器等设备。	2.83
12	万维之旅	1、完成对多通道投影融合系统的研制和开发，对 windows 系统进行融合。 2、利用沉浸式虚拟现实技术，由 3 个面以上（含 3 面）硬质投影墙组成的高度沉浸的虚拟体验环境。参观者可以在被投影墙包围的系统中，近距离接触虚拟三维物体，实时进行跨画面同步交互，或者随意漫游真实的虚拟环境。 3、提供万维之旅互动系统。 4、提供投影仪、电脑、拼接处理器等设备。	248.60	无	-
13	APT 攻击态势	提供 APT 攻击组织及事件展示系统，包括以下功能： 1、APT 攻击组织等级情况统计模块，用矩形树图来展示 APT 攻击组织等级统计情况。 2、APT 攻击组织性质占比统计模块，采用扇形统计图来展示 APT 攻击组织性质占比统计情况。 3、全球 APT 组织分布及事件展示模块，通过 3D 地球的展示方式，应用地图炮来展示 APT 在全球的网络攻击情况。 4、受攻击国家/地区排行统计模块，采用条形统计图来展示 APT 针对不同行业的攻击情况。 5、受攻击行业排行统计模块，采用条形统计图来展示 APT 针对不同行业的攻击情况。 6、海莲花组织针对我国网络攻击事件可视化复现，同时对此事件进行了分析。 7、白象组织针对我国网络攻击事件的可视化复现，同时对此事件进行了分析。 8、方程式组织针对我国网络攻击事件的可视化复现，从地理空间信息和网络拓扑两个角度对方程式攻击事件进行了可视化复现。	226.00	1、提供投影仪、电脑主机等设备。 2、对造型展墙和地台进行加工，包括加钢骨架基础、阻燃板基层等。	20.05
14	电商安全	提供一套软件系统，包括数据采集可视化展示、数据处理可视化展示等功能。	180.80	1、提供电脑主机、触摸屏等硬件。 2、注塑件开模制	28.89

单位：万元 序号	展项名称	公司承担的工作内容	公司分摊的金额（含税）	合肥探奥承担的工作内容	合肥探奥分摊的金额（含税）
				作，木板造型、等工程加工。	
15	信息隐藏与重现	1、完成信息隐藏互动系统的开发和研制。 2、定制多媒体，制作动画介绍什么是信息隐藏。	149.16	1、提供投影仪、电脑主机等设备。 2、加工台体、维修门、扫码器组件，电气控制及制作。	20.89
16	网站防护技术	定制多媒体，包括 10 个内容的 2D 动画视频。	146.90	1、提供感应屏、电脑主机等设备。 2、进行激光切割、异形框架焊接、表面封板、打磨灯槽、折弯焊接处理。	10.29
17	基础设施安全	1、定制触摸屏界面，配合沙盘影片播放，可实现触摸屏交互。提供素材整理编辑、脚本制作、效果渲染、特效输出等影片制作。 2、提供沙盘模型、工程投影机、短焦镜头等设备。	128.72	无	-
18	量子学习空间	提供定制类量子学习机、量子模型、精密直流电压源模型等设备。	119.22	无	-
19	透明机房	提供服务器、工控机、千兆引擎等设备。	105.83	提供灯带、变压器等材料。	0.17
20	共筑网络长城	提供网络长城软件，共包含 20 个分类超过 2,000 道题目，覆盖企业安全、移动安全、通讯安全等。支持在线答题、展示挑战成功效果，支持展示定制长城砖内容。支持多人共筑网络长城。	90.40	1、提供拼接屏、电脑主机等设备。 2、进行图文排版、电气控制及制作。	12.44
21	网络病毒大派对	1、提供角色动画制作，包括《病毒技能大比拼全息成像角色动画 5 套》动画的全片动画渲染、动画特效制作等环节。 2、提供触摸查询软件、同步影像互动软件。 3、提供 LED 屏、反射成像膜、模型灯光系统等设备。	90.40	无	-
22	其他展项	其他	3,437.77	其他	4,445.75
	合计		12,187.50		6,562.50
	比例		65%		35%

上述展项发生采购金额及采购内容如下所示：

单位：万元

序号	展项名称	采购金额	采购内容	成本金额	毛利率
1	赛场	14.46	定位基站、基站嵌入式软件	67.88	94.58%
2	网络教室-网络安全在线云靶场	20.27	台式机	76.36	94.19%
3	数字化展陈	609.10	触控一体机、在线影音互动答题系统	655.96	40.26%
4	网络教室-网安馆专用人才培养靶场	21.73	服务器、台式机	60.61	93.35%
5	网络剧场	361.68	多媒体视频	378.97	6.45%
6	我们网络世界-点阵空间智慧靶场	65.90	多媒体视频	75.39	66.08%
7	网络教室-攻防实战靶场	13.88	台式机、服务器	37.45	93.22%
8	时空长廊-体态互动智慧靶场	1.75	显卡、体感摄像头等	11.2	94.94%
9	网络安全演练	216.81	网络安全演练闯关系统	226.59	1.14%
10	守护网站安全	229.65	展示省行政区网站安全态势感知系统	240.12	2.07%
11	等你来挑战	8.85	显示器、台式机	18.86	91.96%
12	万维之旅	210.38	网络空间立场展示控制系统、电脑、投影机等	220.20	4.29%
13	APT 攻击态势	209.23	威胁情报网关展示系统	218.33	-2.40%
14	电商安全	152.29	电商平台安全可视化展示系统	159.57	6.45%
15	信息隐藏与重现	152.19	多媒体视频、信息隐藏互动系统、新型泄密溯源取证系统	158.19	-12.42%
16	网站防护技术	131.69	多媒体视频	137.60	0.71%
17	基础设施安全	105.52	沙盘触摸屏交互系统、沙盘、触摸一体机等硬件	110.56	6.40%
18	量子学习空间	100.64	模型设计、装修装饰工程、量子学习机	105.18	1.06%
19	透明机房	164.97	服务器、交换机、机柜	168.99	-79.08%
20	共筑网络长城	80.67	企业安全、移动安全答题系统	84.31	1.14%
21	网络病毒大派对	76.50	幻影成像《病毒角色》联动软件、投影机、主机等硬件	80.08	4.39%
22	其他展项	2,715.02	多媒体视频、交互展示类软件、一体机等硬件	2,862.29	10.67%
	合计	5,663.18	-	6,154.68	45.39%

注：成本金额包括采购金额和公司自身实际已发生成本，公司实际已发生成本主要为人工成本。

上述展项毛利率的波动与展项性质、展项是否涉及公司网络靶场有关，具体

如下所示：

展项类型	展项毛利率	毛利率波动原因
与公司网络靶场相关的展项		
网络教室-网络安全在线云靶场	94.19%	展项核心均为公司网络靶场平台技术，不需要大量展示互动类软件或硬件采购，因此具有较高毛利率
赛场	94.58%	
网络教室-网安馆专用人才培养靶场	93.35%	
网络教室-攻防实战靶场	93.22%	
等你来挑战	91.96%	
时空长廊-体态互动智慧靶场	94.94%	
我们·网络·世界-点阵空间智慧靶场	66.08%	
数字化展陈	40.26%	该展项对影音互动答题系统进行了外部采购
与公司其他技术相关的展项		
网络剧场	6.45%	展示类展项，对多媒体视频进行了外部采购，导致成本较高
网站防护技术	0.71%	
基础设施安全	6.40%	展项涉及到大量硬件设备，因此对外采购大量硬件，导致成本较高
量子学习空间	1.06%	
网络安全演练	1.14%	出于时间和展示效果的考虑对展项所需软件进行了外采
守护网站安全	2.07%	
万维之旅	4.29%	
电商安全	6.45%	
共筑网络长城	1.14%	
网络病毒大派对	4.39%	
透明机房	-79.08%	期初展项预算较低，后期客户需求变更涉及到大量硬件设备投入，因此对该展项进行了二次投入
APT 攻击态势	-2.40%	由于客户需求变更进行了展项系统的二次投入

网络安全科技馆项目是联合体成员（公司和合肥探奥）共同与郑州高新产业投资集团有限公司签订合同，最终由郑州高新产业投资集团有限公司直接向公司和合肥探奥进行结算，分别支付相应款项。郑州高新产业投资集团有限公司出具了《关于〈《郑州高新区网络空间安全科技馆展陈建筑设计装修布展一体化项目〉支付比例的说明函》，最终决定向公司支付合同结算价的 65%，向合肥探奥支付

合同结算价的 35%。经走访郑州高新产业投资集团有限公司和合肥探奥，确认科技馆项目的收入分配比例为 65%和 35%。

三、项目验收时点、内容与合同约定的一致性

（一）项目验收时点与合同约定的一致性

网络安全科技馆项目的项目验收时点与合同约定的对比情况如下：

序号	类型	工作内容	合同中的时间安排	实际进展
1	信息化及展品类	信息安全展示软硬件展品设计	2020/4/20-2020/5/20	2020/4/1-2020/9/2
		展品制作（含购置）	2020/4/20-2020/6/15	2020/4/1-2020/9/1
		展品中期检查	2020/5/15-2020/5/20	2020/6/30-2020/7/1
		展品出场验收并运至项目布展现场	2020/6/16-2020/6/30	2020/4/30-2020/9/1
		展品安装及调试	2020/6/26-2020/7/25	2020/8/2-2020/9/1
		数字化解决方案	2020/4/20-2020/7/25	2020/4/20-2020/9/10
		场馆智慧化	2020/5/15-2020/7/25	2020/6/5-2020/9/10
2	建筑设计装修布景类	展馆初步设计	2020/4/1-2020/4/27	2020/4/1-2020/4/9
		展示环境深化设计及布展	2020/4/27-2020/6/30	2020/4/9-2020/9/10
		室内装饰装修工程	2020/4/23-2020/7/1	2020/4/25-2020/9/1
3	项目完工	-	2020/8/10	2020/9/10
4	项目竣工验收	-	2020/9/10	2020/12/25

网络安全科技馆项目涉及展品展项较多，且实施周期短，各项工作交叉进行，实际完成时间与合同存在一定差异。根据甲方规划，该馆首先将服务于 2020 年 9 月开展的国家网络安全宣传周活动。该项目实际于 2020 年 9 月 10 日完工，9 月 14 日如期承办国家网络安全宣传周的开幕活动。因承办活动等原因导致项目验收工作有所推迟，实际于 12 月 25 日完成项目验收工作。

（二）项目验收内容与合同约定的一致性

根据合同约定，合同执行过程中的检查和验收环节包括：投标方案、设计成果专家评审、提交已完成专家评审意见修改的全套设计成果、展品中期检查、展品制作进度和质量检查及出厂验收，展品采用主要设备及材料报审及核验，布展装修材料进场验收，布展隐蔽工程验收，布展装修预制件（含导览和标识装置等）出厂验收，展品竣工验收，以及布展工程竣工验收。合同条款和实际验收情况的

比对如下：

合同内容	实际验收情况
5.1 投标方案 乙方须按甲方的招标要求进行展示初步设计，递交招标文件，提交相应设计文件等资料。	2020年3月24日，公司和合肥探奥向郑州高新产业投资集团有限公司递交投标文件，包括项目设计方案、施工进度计划等。
5.2 设计成果专家评审 乙方按进度计划完成深化设计全部工作，汇报设计成果，提交相应设计文件，接受甲方及甲方组织的专家检查，回答相关质询，确认合格后出施工图纸。	2020年4月9日上午，在河南省郑州市高新区管委会，受郑州市高新产业投资集团委托，成立由学术界、企业界、展陈界9名专家组成的专家组，通过远程视频会议形式对“郑州网络空间科技馆展陈设计方案”进行评审，听取工作汇报和设计方案汇报，调阅了部分深化设计方案、展品展项设计方案和相关佐证材料。专家组通过集体审议，一致同意通过展陈设计方案。
5.3 提交全套设计成果 设计成果是指通过专家评审，并已完成专家评审意见修改的完整设计方案。包含整套空间设计效果图、展品展项效果图、总成图、安装基础图、机械图、电气图，展品多媒体内容脚本、经图审合格的施工图纸等内容；经甲方及甲方组织的专家评审合格后，进入布展施工阶段。	2020年4月，提交完整的设计方案供专家评审，评审合格后开始施工。
5.4 展品中期检查 根据展品专家评审并完成专家评审意见修改的完整设计方案，甲方及甲方组织的专家及监理团队对展品的硬件设备准备及软件系统设计等工作进行检查。确认是否符合设计成果及进度要求，提出整改意见并要求乙方就发现的问题进行整改。	2020年6月30日至7月1日，郑州高新产业投资有限公司、方阵工程咨询有限公司、精诚工程管理有限公司组成检查单位，对网络安全科技馆的展品展项进行中期检查，并制作“展品制作检查记录表”，记录存在的问题和处理意见。每个展项的记录表中均有专家组、展品承包商、监理单位、业主和审计单位的签字。
5.5 展品制作进度和质量检查及出厂验收 5.5.1 甲方按展品制作准备、中期和到货三个阶段对乙方的工作情况进行检查。检查的依据是设计成果和《展品展项深化设计方案》、《展品清单》； 5.5.2 乙方在制作展品过程中，未经甲方批准，不得擅自更改甲方已选定的制作材料和设备，如发现此类问题，乙方除按甲方的要求限期纠正外，还需承担本合同规定的相应的违约责任； 5.5.3 在检查中发现其他不合格项时，乙方应在甲方规定的时限内进行整改和完善； 5.5.4 所有展品展项经甲方和监理单位到货检查合格后，同意展品展项进场； 5.5.5 乙方须按照甲方发出的《展品展项进场通知》，在布展施工单位的统一协商和管理下组织所有展品展项进场。	对项目中的材料、构配件、设备均需填制进场报审表，并将材料清单、质量证明文件和自检结果作为附件，一并提交给监理机构，由方阵工程咨询有限公司出具审查意见。 根据进场报审表、中期检查记录表等文件中的审查意见，公司和合肥探奥及时进行了整改和完善。 所有展品展项均需编制展品进出台账，包含展品名称、组件、数量、单位、包装方式、进场时间等信息。由方阵工程咨询有限公司出具审查意见后，方可进场安装。
5.6 展品采用主要设备及材料报审及核验 展品深化设计完成后提交展品采用主要设备及	展品到货验收后进场时，由监理机构对展品的的主要设备及材料进行核验，并出具审

材料报审，经甲方和监理确认合格后才能使用；展品到货验收后进场时由甲方及监理对展品的主要设备及材料进行核验，必须与报审材料一致，如有改变需出具合理的变更理由，需经甲方确认。	查意见。
5.7 布展装修材料进场验收 材料进场前，乙方向甲方申报材料进场申请，监理对材料进行取样封存。乙方在采购前，其质量、品牌需征得甲方书面签字认可，所有材料均应符合设计要求，并按规定向监理工程师和甲方提供材质合格证书和检验合格证后才能用于工程中。	各批次材料进场前，在方阵工程咨询有限公司的见证下，对混凝土试块、奥松板、阻燃胶合板等进行见证取样，施工中使用的材料均附有材质合格证书和检验检测报告。
5.8 布展隐蔽工程和阶段性工程验收 乙方完成展品安装基础、效果灯光和水、气、网络等外部接口综合布管布线及供配电系统等隐蔽工程或阶段性工程后，须向甲方申请验收，经验收合格后方可进行下一步工序的施工。甲方应在收到乙方验收申请后 3 个日历天内进行验收。	2020 年 5 月至 7 月，分别对轻钢龙骨墙面、铝板墙面、吊顶等隐蔽工程进行验收，形成《隐蔽工程记录表》留档，表中记录隐蔽内容、检查结论和复查结论（如有），并由专业技术负责人、专业质检员、专业工长和专业工程师签字，加盖监理单位公章。
5.9 布展装修预制件出厂验收 乙方在工厂内完成布展装修预制件、剧场和封闭空间的结构件、表演台、观众导览装置、标识装置等的制作后，须向甲方申请验收，经验收合格后方可进行进场安装施工。	对项目中布展装修预制件均需填制进场报审表，并将材料清单、质量证明文件、自检结果和安装基础图作为附件，一并提交给监理单位，由方阵工程咨询有限公司出具审查意见，审查同意后方可进场施工。
5.10 展品竣工验收 5.10.1 竣工验收： 项目完工后，乙方及时提交完整的竣工资料和验收申请，开展竣工验收工作；	2020 年 11 月底至 12 月初，开展各展品的试运行检验工作，制作试运行记录表，记录试运行结果和记录人，并加盖监理公司（方阵工程咨询有限公司）和乙方（北京永信至诚科技股份有限公司、合肥探奥自动化有限公司）专用章。
5.10.2 未通过竣工验收的展品展项，其货物风险责任由乙方承担；	未出现此类问题
5.10.3 甲方收到申请后，应在 10 个工作日内组织验收，超过 10 个工作日未开展验收工作，视为甲方违约，但不免除乙方相应的质量责任；	未出现此类问题
5.10.4 展品展项研发制作验收标准和办法由甲方和监理方另行制定。	甲方组织设立了整体规划与展项内容专项组、软件专项组、多媒体和艺术效果专项组和展项装置专项组，分别制定了展品展项研发制作验收标准和办法。
5.11 项目竣工验收 5.11.1 本项目的试运行期为两个月。	为承接 9 月 14 日开始的国家网络安全周主场馆活动，在 2020 年 9 月 10 日正式完工前，9 月 1 日就开始启动场馆的试运营工作。2020 年 9 月 1 日至 12 月 6 日为网络安全科技馆试运行阶段。试运行期间，累计接待团队 400 余个，总参观人数达到 78,000 余人。
5.11.2 项目完工后 7 个工作日内，乙方自检合格和达到各相关标准后，向监理公司提出竣工申请书；监理公司竣工验收合格后，乙方向甲方	因 2020 年 9 月 14 日至 9 月 20 日，国家网络安全周在网络安全科技馆内举办，展品展项满足运营需求后，场馆进入试运营状

提出竣工验收申请；并提供竣工图及有关竣工文件资料一式叁份（竣工验收时签发的文件除外），甲方在5个日历天内组织竣工验收。	态。2020年12月6日试运营结束后，于12月17日进行现场评审，并顺利验收通过。
5.11.3 验收依据和标准：施工图纸，图纸说明，有关设计变更资料和图纸，装修材料报检报验证明书、技术交底及会议纪要，国家颁布的竣工验收规范、规定，以及专家委员会根据国家有关标准、规范针对本项目特殊子项制订的施工规范及验收标准；	为保证本项目验收的科学性、合理性，设置项目验收专家组，下设4个专项分组（整体规划与展项内容专项组、软件专项组、多媒体和艺术效果专项组和展项装置专项组）、1个综合协调组。针对不同的专项组，也分别制定了相应的验收标准。
5.11.4 由甲方、乙方、监理公司以及政府相关部门等共同组织工程整体验收评定。	2020年12月25日，甲方（郑州高新产业投资集团有限公司）在网络安全科技馆组织召开了“郑州高新区网络空间安全科技馆展陈建筑设计装修布展一体化项目”验收评审会，会议成立了专家组，并邀请政府相关部门（创新发展局、国土规划住建局等行业主管部门）参加监督工作。监理公司（方阵工程咨询有限公司）和乙方（北京永信至诚科技股份有限公司、合肥探奥自动化有限公司）也派人出席会议。
5.11.5 经验收评定，项目质量及项目内容符合合同要求的，甲方、乙方、监理公司均应在项目竣工验收证明书上盖章签字；项目质量不合格或项目内容有尚未完成者，由乙方在商定的期限内进行整改或补充施工后，再进行竣工验收，直至达到完全符合合同要求为止，并按最后验收合格的日期作为竣工日期，由此产生的一切费用和责任均由乙方负责；	2020年12月初，施工单位（公司和合肥探奥）、监理单位（方阵工程咨询有限公司）均在展区验收记录表和展项预验收记录表中签字盖章。 2020年12月17日，甲方（郑州高新产业投资集团有限公司）组织验收评审会，并于2020年12月25日，出具加盖公章的验收评审报告。
5.11.6 甲乙双方应于验收合格后5天内签署项目交接验收证明文件，乙方将场地清理干净后将项目移交给甲方管理；	为承接国家网络安全周的主场馆活动，2020年9月初就开始启动场馆的试运营工作。通过承接学生、企业员工、各级领导的参观来进行压力测试，确保2020年国家网络安全周正常举办。 2020年9月14日至9月20日完成安全周活动后，网络安全科技馆于2020年9月28日正式对公众开放运营。在运营过程中，联合体项目团队与网络安全馆运营团队配合支撑，确保场馆展项可满足运营需求。 顺利试运营3个月后，于2020年12月份正式启动验收工作。
5.11.7 项目未竣工验收，甲方若需提前使用，需经乙方同意，使用期间内甲方承诺不损坏场馆装修及产品设施。如若涉及损毁情况而产生的费用问题，由甲乙双方另行协商。	在试运营过程中，如果遇到展项故障的情况，通过监控录像查阅分析，运营公司与项目联合体根据问题原因，明确职责和分工。如因人为因素造成展项损坏由运营公司进行维修，如因展项质量问题则由项目联合体负责维修。
5.11.8 甲方不能因展品原因（如部分展品未进场或未完成安装、调试等）而拒绝对乙方进行布展验收。因展品原因导致乙方部分设计或施工	因2020年9月14日至9月20日国家网络安全周在网络安全科技馆内举办，场馆提前进入运营状态，展品展项满足运营需求，

工作无法按期完成时，甲方需按期对乙方已完成部分预验收。	故试运营结束后直接进行了验收工作，不存在部分预验收的情况，不存在展品未进场或未完成安装、调试进行验收的情形
-----------------------------	---

网络安全科技馆项目的验收时点、验收内容，和合同约定的主体内容基本保持一致。该项目于 12 月 17 日进行现场评审，并于 12 月 25 日出具加盖公章的验收评审报告。实际施工过程中，公司提交了合同中所要求的项目管理文件、技术文件、项目物资出厂质量证明及进场检测文件、展品中期检查记录、项目质量验收及试验记录文件等，并且顺利通过最终验收。

四、回款时点、金额与合同约定的匹配性

根据合同约定，发行人应收取合同价款共计 12,187.50 万元（包含增值税），其中，截至 2021 年 10 月末，公司对设计阶段至验收阶段的 11,843.81 万元合同价款具备收款权利，已将该等款项全部收回。其余 343.69 万元为质保金，由于质保金尚未到期，客户尚不需要履行付款义务。合同的具体结算约定及实际回款情况如下：

单位：万元

阶段	结算约定	应收取款项时间	应收取金额	实际回款时间及实际回款金额	实际回款金额与合同约定金额差异
设计阶段	设计费为合同金额的 6%。合同签订后 5 个工作日内，甲方支付设计费总额的 70%，施工图纸提交后 5 个工作日内，甲方支付设计费总额的 30%	2020 年 5 月	731.25	2020 年 6 月至 11 月：9,697.09 万元	-
布展施工和展品制作阶段	合同签订后 10 个工作日内，甲方支付扣除项目设计费后中标价的 20%	2020 年 5 月	2,291.25		
	展品中期检查后发现问题并完成整改的 10 个工作日内，甲方支付扣除设计费后总金额的 50%	2020 年 7 月	3,436.88		
	展品完成制作，经甲方、专家及监理审核确认符合要求且无质量问题后 5 个工作日内，甲方支付扣除设计费后总金额的 75%	2020 年 9 月	2,864.06		
	展品及布展工程完成后 10 个工作日内，甲方支付扣除设计费后总金额的 85%	2020 年 9 月	1,145.63	2021 年 3 月至 10 月：2,146.72 万	
项目竣工验收	项目竣工验收合格后 10 个工作日内，甲方支付扣	2021 年 1 月	1,374.75		

	除设计费后总金额的97%			元	
设计阶段至项目验收阶段合计	-	-	11,843.81	11,843.81	-
质保期	质保金金额为合同价款扣除设计费后的3%。项目竣工后24个月为质保期，质保期结束且产品达到保修条款要求后，甲方退还质保金	2022年	343.69	根据合同约定，质保期尚未到期，故甲方尚未支付相应款项	不适用，客户尚不需要履行付款义务

如上表所示，截至2021年10月末，公司已将设计阶段至项目验收阶段应收取的合同价款全部收回，项目回款不存在异常。对于尚未收回的343.69万元质保金，由于质保期尚未到期，故相关款项尚未收回具有合理性。

(4) 软件、服务、多媒体、设备收入的划分依据、交付成果，合同中各部分金额的约定情况；发行人在该项目中对外采购的具体内容及主要供应商，专业技术服务费采购金额较大的原因，发行人实际提供的服务内容，将对外采购部分产生的收入作为核心技术收入的原因；

一、网络安全科技馆建设项目中软件、服务、多媒体、设备收入的划分依据、交付成果，合同中各部分金额的约定情况

(一) 收入等约定情况

网络安全科技馆项目中软件、服务、多媒体及设备收入的划分依据为项目实际交付过程中所提供产品及服务的类型及甲方确认的结算清单，所交付的成果分别为软件使用权、展品设计及组织管理服务、多媒体产品和硬件展品。

网络安全科技馆项目合同中对各部分金额的约定及本公司的收入情况如下：

单位：万元

收入划分	合同约定金额 (含税)	合肥探奥承担金额(含税)	收入金额 (含税)	收入金额 (不含税)	其中：计入核心技术产生收入(不含税)
软件收入	7,858.56	236.77	7,621.79	7,026.62	4,921.71
服务收入	5,341.27	2,965.17	2,376.10	2,215.46	700.78
多媒体收入	1,545.10	-	1,545.10	1,457.64	240.57
设备收入	4,005.08	3,360.57	644.51	570.36	60.56
合计	18,750.00	6,562.50	12,187.50	11,270.09	5,923.62

注释：多媒体收入属于服务收入，由于多媒体收入较高，为投资者充分理解，将多媒体

收入分开列示。

网络安全科技馆建设项目中软件、服务、多媒体、设备收入金额分别为 7,026.62 万元、2,215.46 万元、1,457.64 万元和 570.36 万元，占比分别为 62.35%、19.66%、12.93%和 5.06%。网络安全科技馆项目收入的划分依据为项目实际建设过程中所提供产品及服务的类型及甲方确定的结算清单。

软件收入指的是公司在网络安全科技馆项目中提供的涉及软件技术的部分展品，该部分确认收入金额为 7,026.62 万元，交付成果为软件，公司提供相关软件，软件灌装到相关硬件设备中使用，与网络靶场相关展项的软件收入计入了核心技术产生的收入中，金额为 4,921.71 万元，占软件收入的 70.04%。网络安全科技馆项目属于在某一时点履行的履约义务，在科技馆项目所有展品的控制权已经转移，产品已经提供并安装调试完成，取得客户确认的项目整体验收报告，且相关的经济利益很可能流入时确认项目全部收入，发行人于 2020 年年底确认了收入。合同约定金额与公司收入结算金额存在差异，差异系联合体合肥探奥所承担的智能建筑相关的软件对价。

服务收入指的是公司在网络安全科技馆项目中承担的展品服务、管理服务和设计服务，该部分确认收入金额为 2,215.46 万元。服务成果主要系展品的设计、项目现场的组织和管理等，与网络靶场相关展项的设计集成和管理等收入计入了核心技术产生的收入中，金额为 700.78 万元，占服务收入的 31.63%。合同约定金额与公司收入结算金额存在差异，差异系联合体合肥探奥所承担的基础装修费中装修服务的对价。

多媒体收入指的是公司在网络安全科技馆项目中承担的多媒体展品的设计和制作，该部分确认收入金额为 1,457.64 万元，交付成果系多媒体产品的所有权，与网络靶场相关展项的多媒体收入计入了核心技术产生的收入中，金额为 240.57 万元，占多媒体收入的 16.50%。多媒体收入包括自制多媒体收入 405.75 万元和委托制作多媒体收入 1,051.89 万元。自制多媒体收入主要是公司根据展项的主题和具体要求制作对应的多媒体视频；委托制作多媒体中公司总体主导，包含策划、创意、设计等内容，具体制作公司交予多媒体供应商负责。该部分服务均由公司独立交付，不存在公司与联合体合肥探奥分摊合同收入的情况。

设备收入指的是公司在网络安全科技馆项目中承担的硬件展品的购买及制

作，该部分确认收入金额为 570.36 万元，交付成果系硬件展品的所有权，与网络靶场相关展项的设备收入计入了核心技术产生的收入中，金额为 60.56 万元，占设备收入的 10.62%。合同约定金额与收入结算金额存在差异，差异系联合体合肥探奥所承担的基础装修中与装修设备投入的对价。

（二）核心技术产生收入及主营业务收入情况

公司属于网络安全企业，主要以项目制形式开展业务，“网络安全科技馆”项目是独立的一个项目，公司以整体项目对客户负责，虽然网络安全科技馆共分为多个展项，各个展项的收入可以依据结算单进行划分，但是各个展项并不是独立存在，公司无法以单个或者多个展项对客户负责，整个项目的验收亦是整体验收。

网络安全科技馆项目是依托公司自身核心技术而形成的系统性、不可分割的整体解决方案，但是该项目收入 11,270.09 万元，占 2020 年公司营业收入总额的比例为 38.64%，占比较高。为方便投资者理解，且基于谨慎性考虑，公司依据结算单对各个展项的收入进行了细分，主要分为网络靶场类展项、其他技术类展项两类，其中公司将网络靶场展项列入核心技术产生的收入中。

具体展项中，公司以各个展项对客户负责，主要核心为公司网络靶场，网络靶场的核心技术是发行人承接该项目的基础，是客户评判项目质量的重要指标。公司根据客户需要搭配定制开发的软件产品或外购的软硬件产品，实现系统性功能，整体交付给客户。网络靶场类展项中，外采设备产生的收入为 60.56 万元、外采定制软件产品产生收入为 589.62 万、外采多媒体产品产生收入为 90.57 万元，合计 740.75 万元，占网络靶场类展项收入的 12.51%。外采的产品或服务是在公司基于整个项目的设计理念，在公司的要求下外采的产品或服务，而非市场上本身存在的通用产品，外采的产品或服务为公司核心技术产品的辅助部分配套向客户提供，与公司的核心产品作为整体起到作用，无法单独使用，在整体项目作用中仅起到辅助作用，因此计算核心技术收入时，无需剔除外采产生的收入。

科创板上市公司中科通达（688038）、长威科技（已提交注册）、和达科技（688296）、星球石墨（688633）在计算核心技术产生收入时将外采的部分作为项目的成本，作为项目的组成部分，未在核心技术收入计算时剔除，与公司类似。

截至目前，科创板上市公司中网络安全相关行业公司，核心技术收入占主营

业务收入比例情况如下：

序号	公司名称	注册时间	最近 1 期	报告期第 3 年	报告期第 2 年	报告期第 1 年
1	安博通	2019.8	99.72%	99.79%	93.71%	90.83%
2	山石网科	2019.9	97.24%	97.28%	98.09%	98.71%
3	安恒信息	2019.10	93.51%	90.99%	90.75%	88.20%
4	云涌科技	2020.6	-	98.32%	96.88%	92.97%
5	奇安信	2020.7	-	77.47%	75.55%	77.04%
6	信安世纪	2021.3	98.33%	95.91%	94.23%	93.77%
7	纬德信息	2021.12	99.87%	99.69%	99.30%	98.80%
8	亚信安全	已提交注册	91.39%	91.61%	91.12%	89.56%
平均			96.68%	93.88%	92.45%	91.24%
发行人			96.03%	78.43%	93.49%	94.61%

由上表可见，公司核心技术产生收入占比与同行业公司不存在重大差异。

其他技术类展项中，虽然未列为核心技术产生的收入，但都是网络安全行业的范畴，与网络靶场类展项形成有效互补，全面覆盖网络空间安全体系，构建成完整的科技馆，是整体项目不可或缺的一部分，客户就项目的整体实施效果是否符合约定进行验收，公司需就项目整体运行的有效性向客户负责。此类展项属于公司为客户提供整体项目的主营业务范畴，公司将其列为主营业务收入符合业务实质。

二、公司在网络安全科技馆建设项目中对外采购的具体内容及主要供应商，专业技术服务费采购金额较大的原因，公司实际提供的服务内容，将对外采购部分产生的收入作为核心技术收入的原因

（一）网络安全科技馆建设项目中对外采购的具体内容及主要供应商，专业技术服务费采购金额较大的原因

公司网络安全科技馆建设项目的供应商主要提供多媒体类展品的制作、展陈技术的开发、硬件设备及装修、软硬件一体化服务、软件展品辅助技术的开发等服务。公司对外进行采购主要出于以下几点考虑：

1、由于公司不具备多媒体视频的制作能力、硬件设备生产能力，公司对实物类展品按照项目需求进行开发设计，确定技术参数后委托第三方公司进行外包制作；

2、公司基于成本效益的考虑，将部分重复性、机械性、低附加值的简单的基础性软件开发以及技术服务工作委托给第三方公司执行；

3、公司基于项目的整体展示效果，公司网络安全科技馆项目对部分不涉及公司核心技术的展品及技术进行外包，如与百度网讯、观脉科技、阿里云计算等著名网络安全公司发生的外包类采购。

综上，公司基于网络安全科技馆项目的需求、成本效益、展示效果等考虑，对外的技术服务采购金额较大。

网络安全科技馆项目中采购的主要供应商及采购情况如下：

单位：万元

序号	供应商	合同内容	采购分类	采购金额	占比
1	随锐科技集团股份有限公司	科技馆意识闯关、安全射击等趣味游戏模块开发	展陈技术的开发	589.62	10.41%
2	北京鹏途腾飞科技有限公司	动画视频制作及剪辑	多媒体类展品的制作	367.92	6.50%
3	北京中顺诚科技有限公司	动画影片制作	多媒体类展品的制作	358.49	6.33%
4	北京百度网讯科技有限公司	科技馆 AI 手势识别、AI 图片识别等部分展项的制作	展陈技术的开发	331.49	5.85%
5	上海齐耘文化展览有限公司	“魔鬼病毒大派对”展项组软硬件、“万维之旅-沉浸式互动投影空间”硬件设备采购安装、新增22个展项设计及其深化平面上墙图文设计	软硬件一体化服务	320.26	5.66%
6	观脉科技（北京）有限公司	网安科技馆 APT 攻击态势展示-威胁情报网关系统开发	展陈技术的开发	279.18	4.93%
7	阿里云计算有限公司	魔镜、云安全风险、电商安全展项的软件开发	展陈技术的开发	254.72	4.50%
8	河南辰泰电子科技有限公司	中国网络安全科技馆智能化系统工程施工	软硬件一体化服务	252.78	4.46%
9	上海且听网络技术服务中心	守护网站安全模块软件开发	展陈技术的开发	227.72	4.02%
10	北京坤元和讯技术有限公司	网络安全演练系统开发	展陈技术的开发	215.00	3.80%
11	北京恒辉国信科技有限公司	网站安全防护、明日之前展项视频录制制作	多媒体类展品的制作	180.00	3.18%

12	西安再想想网络科技有限公司	网安科技馆“找到特洛伊”展项软件开发	展陈技术的开发	174.53	3.08%
13	中国科学技术大学	基于用户体验的网络安全人才培养展项设计方案研究/基于用户体验要素模型的郑州网络安全科技馆设计方案研究	软件展品辅助技术的开发等服务	165.05	2.91%
14	北京惠智普耀科技有限公司	测试数据支撑服务、电子数据鉴定服务和电子数据清洗服务	软件展品辅助技术的开发等服务	160.38	2.83%
15	北京华海志成科技有限公司	三维动画制作	多媒体类展品的制作	155.66	2.75%
16	杭州安恒信息技术股份有限公司	国家关键信息基础设施安全、智能工业系统安全、基础设施安全展项制作	软硬件一体化服务	128.55	2.27%
17	河南灵创电子科技有限公司	仿冒电话、绵羊墙、短消息与安全等 7 个展项的制作	软硬件一体化服务	120.80	2.13%
18	四川科瑞软件有限责任公司	屏拍溯源、纸中窥密、音信无痕软件的开发	展陈技术的开发	113.21	2.00%
合计				4,395.35	77.61%

（二）网络安全科技馆建设项目公司实际提供的服务内容，将对外采购部分产生的收入作为核心技术收入的原因

根据网络安全科技馆项目的相关合同约定，科技馆项目是一个展陈建筑设计装修布展一体化项目，因此公司主要承担网络安全科技馆项目的展品设计、产品制作、产品软件开发及配套硬件采购等工作。

网络安全科技馆中展项可以分为两部分：核心展项与辅助类展项。其中核心展项如网络教室、等你来挑战、赛场等展项以公司自有的技术和产品为基础，根据网络安全科技馆展览需求、赛事需求等进行的相关定制研发。以网络教室-网络安全在线云靶场展项为例，公司以人才培养靶场为基础，实现了网络安全实验室靶场系统、虚拟仿真分系统、比武竞赛分系统、安全实训分系统、综合管理分系统、软件资源包费用、精品课程定制等系统部署，满足了展项所要求的学习、比赛、培训等需求。因此此类展项的核心要素、技术、内容等均依赖于公司既有的历史产品及技术。

同时，该项目工期较为紧迫，公司对部分展项的功能模块进行了拆解，并将设计好的方案及辅助类展项进行了外包，使得其使用流程、展示效果、输出的安

全知识内容、实现体验效果、数据分析效果等在较短时间内达到预期水平。

综上所述，公司网络安全科技馆项目存在一定金额的对外采购，主要是基于专业技术的可视化、可理解性的需求和成本效益的要求。网络安全科技馆项目中的攻防实战靶场、赛场等核心展项均为公司基于自有的专利技术、软件著作权及其他核心技术进行设计并完成，同时对非公司技术方向的展示辅助类展项进行了外包。基于谨慎性考虑，发行人在核心技术产生的收入中剔除了网络安全科技馆中非公司网络靶场相关的展项产生的收入。

(5) 郑州天健网安技术有限公司后续的运营方式，向发行人后续采购的内容。

一、郑州天健网安技术有限公司后续的运营方式

天健网安是公司的参股公司，其控股股东为郑州高新智慧城市运营集团有限公司，实控人为郑州高新技术产业开发区管理委员会。郑州高新技术产业开发区管理委员会是郑州市政府的派出机构，受郑州市人民政府委托，对高新技术产业开发区实行统一领导和管理。

2020 年 8 月，为保证网络安全科技馆的顺利运营及开发，郑州高新智慧城市运营集团有限公司、即刻点石、合肥探奥自动化有限公司和郑州信大先进技术研究联合设立了郑州天健网安技术有限公司，因此天健网安定位于为网络安全科技馆提供运营服务的企业，公司作为天健网安的股东行使股东权利。

天健网安采用市场化运营方式向网络安全科技馆提供运营服务，获取相应的收入，该部分收入是天健网安主要收入。

二、郑州天健网安技术有限公司后续向公司进行的采购

截至 2021 年 11 月 30 日，天健网安就“行走的网络安全科技馆”展项系统开发项目向公司进行了两笔采购，采购金额合计为 150.00 万元，合同内容包括 WIFI 绵羊墙互动体验系统、网络信息透明人系统、中奖短信诈骗系统、ETC 盗刷体验系统、AI 换脸术体验系统等项目。

【核查程序】

保荐机构、申报会计师及发行人律师执行了以下核查程序：

1、取得网络安全科技馆项目的采购清单、采购合同，访谈该项目负责人，了解相关采购内容与公司主营业务的相关性；检查该项目招投标资料、销售合同、

验收报告，了解网络安全科技馆的交付形态；实地走访网络安全科技馆，访谈项目经理，销售总监，了解公司将该项目归入网络靶场和人才培养的依据和公司对未来科技馆业务的规划，了解此类业务的持续性；

2、获取网络安全科技馆项目的展项清单、访谈项目负责人及相关技术人员，了解展品展项与发行人主营业务关系以及核心技术等在相关展项中的具体应用；

3、取得并检查公司在手订单、相关合同及合同履行情况，访谈总经理、销售总监和财务总监，了解公司目前正在洽谈的商机合同的客户及金额，结合未来行业市场前景及规划，分析公司业绩是否具有可持续性，判断公司是否符合上市标准；

4、取得网络安全科技馆项目销售合同、中标通知书、各阶段验收报告，通过对网络安全科技馆项目的客户以走访、函证的方式向客户确认项目验收时间，结合销售合同、招投标文件分析该项目是否存在收入确认跨期；对该项目客户郑州高新产业投资集团有限公司及联合体方合肥探奥进行访谈了解收入金额调整原因，取得项目过程性资料结合公司项目工作量进行检查，判断项目验收时点、项目实施内容是否与合同约定一致；获取网络安全科技馆项目的回款凭证，核查相关回取得并检查网络安全科技馆结算单中软件、服务、多媒体设备收入的合同约定情况；获取了网络安全科技馆建设项目的供应商清单，取得相关交易合同，访谈项目负责人，了解交易背景和原因；检查相关交易的会计核算情况；结合《企业会计准则》等，分析网络安全科技馆项目收入采用总额法核算的合理性；

6、访谈天健网安总经理，了解该公司后续运营方式，了解公司向天健网安采购的相关内容，取得相关交易合同，检查是否存在异常；

7、获取网络安全科技馆项目的采购明细，核查采购情况与各展项的匹配关系；访谈发行人总经理，了解对外采购的原因及合理性。

8、访谈发行人总经理及财务总监，了解网络安全科技馆项目核心技术产生的收入的划分依据，了解外采产品或服务的相关展项是否应用了发行人核心技术；查询科创板上市公司及在审企业案例，核查其划分核心技术产生收入的依据是否与发行人具有可比性，进而核查发行人对核心技术产生收入的划分方式是否符合行业惯例。

【核查意见】

经核查，保荐机构及申报会计师认为：

1、网络安全科技馆项目中，发行人重点支撑了网络教室、赛场、等你来挑战，以及数字化展陈等展品，与公司主要的技术与产品直接相关，该项目收入与公司的主营业务具有相关性；公司已对科技馆类项目进行了规划和部署，截至2021年11月30日已签订了部分项目合同；

2、截至2021年11月30日，公司在手订单金额达到22,854.61万元，在手订单较为充裕，当前业务拓展情况良好，业务开展的可持续性较好；

3、网络安全科技馆项目的合同工作内容、项目内容、合同工期、质量标准等内容与招投标文件一致，根据建设中的业主和专家组的意见实际展项内容存在一定的调整，在展陈行业，实际建造中的展项细节调整属于常见现象，网络安全科技馆项目的合同主要内容与招投标文件基本一致；收入金额调整原因、过程、与工作量匹配关系分析符合实际情况，验收时点、验收内容与合同约定内容一致；网络安全科技馆项目的实际回款情况受客户付款审批复杂等因素影响，与合同约定未形成一一匹配关系，但截至2021年10月末，回款金额符合合同约定；

4、网络安全科技馆项目软件、服务、多媒体、设备收入的划分依据系《网络安全科技馆结算单》，公司网络安全科技馆项目存在一定金额的对外采购，主要是基于专业技术的可视化、可理解性的需求和成本效益的要求；网络安全科技馆项目整体由公司基于自有的专利技术、软件著作权及其他核心技术进行设计并提供相应的整体解决方案及集成服务。因外部采购金额较大，公司在核心技术产生的收入中剔除了网络安全科技馆外部采购产生的收入；网络安全科技馆项目收入采用总额法确认具有合理性，符合《企业会计准则》规定；

5、天健网安后续的运营受郑州高新技术产业开发区管理委员会的统一领导和管理，其截至2021年11月30日向公司采购的内容主要系网络安全科技馆的增量展项。

经核查，发行人律师认为：

1、网络安全科技馆项目的展项与发行人主营业务密切相关，网络安全科技馆项目的展项运用了发行人的软件著作权、专利以及核心技术。网络安全科技馆项目与发行人其他网络安全产品在交付形态上均主要表现为纯软件或软硬件一体化产品。网络安全科技馆项目收入归入网络靶场系列产品系按照靶场的应用场

景来分类。

综上所述，网络安全科技馆项目是公司未来发展战略规划中必要的产品组成部分。虽然全国性单体大规模的科技馆类项目在短期内可持续发生尚存在不确定性，但公司已在组织架构、研发、市场开拓等方面对该类业务进行了规划和部署，密切跟踪市场中的商机项目，并且已签订了部分项目合同。

2、发行人网络靶场系列产品的收入稳步提升，网络靶场系列产品的平均单价呈上升趋势。发行人网络靶场系列产品在行业市场中具有先发优势，在多个行业具有广阔市场机会。发行人运作大项目的能力增强，市场需求不断增加。

截至 2021 年 11 月 30 日，发行人在手订单金额达到 22,854.61 万元，发行人的在手订单充裕，业务扩展情况良好，发行人业绩具有可持续性，发行人持续符合上市标准。

4、关于行业竞争情况及同行业公司对比

根据申报材料：（1）根据数世咨询发布的《中国网络安全百强报告（2021）》显示，综合实力百强企业分为领军者、竞争者和挑战者，其中领军者 32 家、竞争者 38 家、挑战者 30 家，发行人入选竞争者；（2）在安全企业级培训服务市场，发行人以 23.35% 的市场份额，位居该细分领域第一名；（3）在网络安全竞赛服务方面，发行人具有明显的领先地位；2018 年 10 月 25 日，中科合创（北京）科技成果评价中心组织院士对公司的“城市网络靶场构建技术及应用”进行集中评定，认为“该项目达到国内领先水平”；（4）启明星辰、奇安信等公司为同行业可比公司，与同行业相比，公司收入、利润规模较小，公司认为其竞争劣势为融资渠道匮乏、收费模式单一。

请发行人披露：（1）按照主要产品量化分析发行人与同行业可比公司核心技术指标的对比情况，并论证其相关技术的先进性；（2）结合公司主要产品所处细分行业的市场竞争格局、市场占有率、与主要竞争对手在产品布局、技术水平、下游应用领域、销售渠道等方面的差异，客观披露发行人竞争劣势和技术先进性。

请发行人说明：（1）安全企业级培训服务市场的市场空间；（2）发行人在网络安全竞赛服务方面具有明显的领先地位的体现，2018 年“城市网络靶场构建技术及应用”评定结果作为发行人技术达到国内领先水平的依据是否充分。

请保荐机构对上述事项进行核查，并发表明确意见。

【回复】

请发行人披露：

(1) 按照主要产品量化分析发行人与同行业可比公司核心技术指标的对比情况，并论证其相关技术的先进性；

发行人已在招股说明书“第六节 业务和技术”之“二、发行人所处行业基本情况及其竞争状况”之“（四）发行人产品或服务的市场地位、技术水平及特点、行业内主要企业、竞争优势与劣势、行业发展态势、面临的机遇与挑战，以及报告期内的变化和趋势”之“3、产业竞争情况及行业内主要企业情况”之“（3）同行业公司对比情况”补充披露如下：

公司主要产品依赖于网络靶场技术，主要体现为平行仿真和网络攻防，尚无权威机构出台行业通用技术指标评价标准，同行业公司尚未披露网络靶场的详细信息，因此无法直接进行对比，在数据可获得的前提下，从以下几个方面论证公司相关技术的先进性。

序号	方面	发行人情况简介
1	科研成果评定方面	被认定“该项目达到国内领先水平”
2	获奖方面	“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获2019年度北京市科学技术奖（科学技术进步奖）一等奖。这是网络靶场技术首次获得此奖。
3	行业研究报告方面	在数世咨询发布的《网络靶场能力指南》报告中，发行人网络靶场在应用创新力和市场执行力维度均位列行业第一。
4	比赛印证	由公安部主导的“网鼎杯”是国内影响力最大的网络安全比赛之一，大赛规模屡创纪录。两届“网鼎杯”均使用公司网络靶场平台完成。
5	鹏城实验室	经中央批准成立的鹏城实验室，主要研究项目之一为网络靶场，鹏城网络靶场合作方较多，主要为四川大学、武汉大学、中科院信工所等高校或科研机构，以及中国联通、宁波国电、南方电网等国家重点基础设施单位，网络安全公司主要为发行人和启明星辰。
6	核心技术指标方面	鹏城网络靶场的介绍的在目标网络规模（百万级节点）及其灵活部署，网络安全事件准确检测（有效性到90%以上），网络实验任务并发数（1000个实验并发）等方面达到了世界领先水平。 公司的“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获2019年度北京市科学技术奖（科学技术进步奖）一等奖，部分技术指标也可以达到上述要求。
7	团队方面	公司参与起草或修订三项网络安全国家标准。2016年至今，公司团队连续多年参加由公安部主办的国家级网络安全实战攻防演习，曾连续三年荣获企业队第一名。

8	行业案例方面	2020年首家网络安全科技馆落户河南郑州，并成为2020年国家网络安全宣传周的核心场馆、“强网杯”全国网络安全挑战赛的永久赛场，公司负责展陈的策划、设计、统筹及建设。
---	--------	---

一、科研成果评定方面

2018年10月25日，中科合创（北京）科技成果评价中心组织院士等专家对公司的“城市网络靶场构建技术及应用”进行集中评定，认定“该项目达到国内领先水平”。

中科合创(北京)科技成果评价中心是经科技部有关部门批准成立的全国第一家第三方专业科技成果评价机构，是工信部认定的国家军民融合科技评估机构，也是全国唯一一家与公安部科技信息所联合开展全国公安系统和社会公共安全领域科技成果评价的第三方专业评价机构。

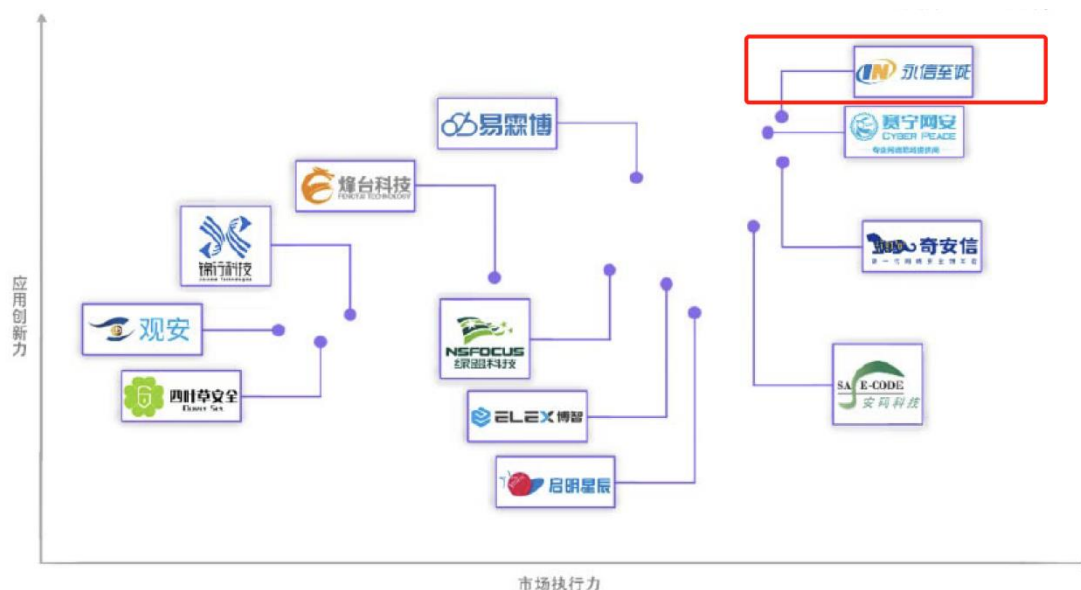
二、获奖方面

公司作为第一完成人的“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获2019年度北京市科学技术奖（科学技术进步奖）一等奖。这是网络靶场技术首次获得此奖。北京市科学技术奖过去五年网络安全企业获奖情况如下：

奖项（北京市）	获奖编号	项目名称	网安企业
科技进步一等奖	2019-J02-1-02	基于平行仿真的大规模网络靶场构建技术及应用	发行人
科技进步二等奖	2019-J02-2-03	工业互联网安全监测运营技术与应用	奇安信
科学技术二等奖	2018 计-2-003	网络空间大规模关键信息基础设施安全态势感知关键技术研究与应用	绿盟科技
科学技术三等奖	2018 计-3-004	网络安全威胁态势感知和应急处置技术研发及产业化	奇安信
科学技术二等奖	2016 计-2-001	面向电力信息系统的安全可控性仿真验证体系研究与应用	启明星辰
科学技术三等奖	2016 计-3-003	基于大数据分析的企业内网的未知威胁防御系统的研发和应用	北京奇虎科技有限公司、北京奇安信科技有限公司

三、行业研究报告方面

在数世咨询发布的《网络靶场能力指南》报告中，发行人网络靶场在应用创新力和市场执行力维度均位列行业第一。



四、比赛印证

由公安部主导的“网鼎杯”是国内影响力最大的网络安全比赛之一，2018年首届“网鼎杯”，7,000多支队伍、2.25万人参赛，创造了最大规模网络安全赛事纪录，2020年第二届“网鼎杯”共有14,724支战队，39,613人参加，大赛规模再次打破纪录。两届“网鼎杯”均使用公司网络靶场平台完成。

五、鹏城实验室

经中央批准成立的鹏城实验室，主要研究项目之一为网络靶场，发行人与各大高校、企业作为鹏城网络靶场的分靶场，支持鹏城网络靶场的建设工作，鹏城网络靶场合作方较多，主要为四川大学、武汉大学、中科院信工所等高校或科研机构，以及中国联通、宁波国电、南方电网等国家重点基础设施单位，网络安全公司主要为发行人和启明星辰。



六、核心技术指标方面

公司网络靶场主要指标如下所示：

靶场相关能力	具体情况
支持的靶场类型	赛事演练靶场； 人才培养靶场； 智慧城市安全测试靶场； 案件线索追踪实战靶场； 业务模拟靶场； 人工智能攻防靶场； 复杂业务安全推演靶场； 综合场景应用靶场（涵盖科技馆、人才基地等）。
仿真及虚拟化能力	全自主研发的春秋云靶场专用管理平台； 支持 KVM、docker、VMware、Xen、QEMU 等多种类型的虚拟机导入，兼容 OpenStack 等云平台接口； 支持全虚拟机、容器虚拟化、数字仿真、模拟仿真、协议仿真、流量仿真六维融合仿真技术； 支持与终端设备、路由交换设备、网络设备等多种类型的实体设备结合构建隔离的软件定义隔离网络，并支持自动化部署脚本进行快速状态恢复； 支持基于流量、自动化脚本等进行业务或特定的行为仿真。
已公开验证过的最大节点部署规模	2020 年“网鼎杯”半决赛现场，单一场景 8000+全虚拟机节点
可支持的最大节点部署规模	百万级节点多集群联动
千级别节点实例化时间	分钟级
单虚拟机节点实例化时间	秒级
并发及接入能力	支持多种类型的靶场任务并发下发，所有任务数据及虚拟化场景严格隔离；

	支持单任务或多任务统一动态导调，支持动态数据采集及实时效能评估； 每个任务均支持攻击测试、防御、监管、厂商、供应链、普通应用者等多种角色按不同权限接入场景实时互动； 支持个人终端、VPN 远程、靶场操作虚拟机等各类接入模式。
成功支持基于网络靶场的省部级以上竞赛及演习案例	网鼎杯、强网杯、护网杯、全国信息安全竞赛、巅峰极客网络安全大赛、粤盾演习、DefCon 中国赛、黄鹤杯 RHG 人工智能安全大赛等。
靶标资源	百万级中低交互节点集群靶标； 操作系统虚拟机靶标 1500+； 高交互靶标 5000+； CVE 漏洞验证靶标 1000+； 漏洞知识库 20 万+； 各类漏洞环境 10000+； 高交互仿真场景 800+； 行业及城市级仿真场景 100+。
多级靶场级联或其他平台兼容性	支持春秋云境靶场多级级联； 标准数据接口支持与其他网络靶场或管理系统进行兼容。

七、团队方面

公司董事长蔡晶晶先生从事网络安全服务行业超过十五年，是国内资深的网络安全专家之一，正高级工程师，也是国家“万人计划”、第三届“杰出工程师”、“2018国家网络安全优秀人才”奖的获得者。

公司核心团队主要成员是国内最早的一批网络安全技术专家，均拥有多年的专业网络安全从业经历。公司拥有自主知识产权的网络安全产品以及专业的安全技术研究和团队。公司参与起草或修订三项网络安全国家标准。

2016年至今，公司团队连续多年参加由公安部主办的国家级网络安全实战攻防演习，曾连续三年荣获企业队第一名。

八、行业案例方面

2020年首家网络安全科技馆落户河南郑州，并成为2020年国家网络安全宣传周的核心场馆、“强网杯”全国网络安全挑战赛的永久赛场，公司负责展陈的策划、设计、统筹及建设。网络安全科技馆已成功运营网络安全相关活动百余场，已接待15万+观众参观体验。

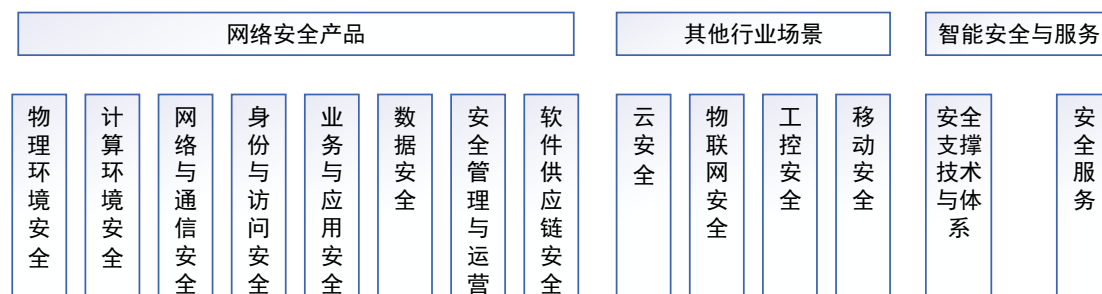
(2) 结合公司主要产品所处细分行业的市场竞争格局、市场占有率、与主要竞争对手在产品布局、技术水平、下游应用领域、销售渠道等方面的差异，客观披露发行人竞争劣势和技术先进性。

一、竞争劣势

近年来，我国网络安全行业市场增长较快，参与厂商众多。2018 年我国共

有 2,898 家从事网络安全业务的企业。由于网络安全行业市场细分程度较高，目前网络安全产品的细分领域多达百余个，不同细分市场的领先厂商不尽相同，市场集中度较低，不同的细分领域存在不同的优势厂商。

参考安全牛网络安全行业全景图，网络安全行业主要可进行以下划分：



根据安全牛网络安全行业全景图，一级分类达 14 类（如上图所示），二级分类众多，达 105 种领域，以下为同行业上市公司涉及领域：

单位：万元

上市公司	2020 年收入	涉及领域	下游应用领域
启明星辰	364,674.53	上网行为管理、下一代防火墙、主机入侵防御、云平台安全运营等 55 个领域	政府机关、电信、金融行业和大型国有企业等
美亚柏科	238,609.83	身份认证、权限管理、备份与恢复、零信任等 14 个领域	主要用户群体为国内各级司法机关、行政执法部门、政务监管部门等
绿盟科技	201,004.43	上网行为管理、网络隔离、网络入侵防范、下一代防火墙、5G 安全、终端安全管理等 62 个领域	以政府、电信运营商、金融、能源、互联网领域内的企业级客户为主
深信服	545,839.52	通信安全、流量检测与管理、上网行为管理、AI 防火墙、链路负载均衡、安全路由器/交换机等 47 个领域	企业、政府及事业单位、金融及其他行业等
安恒信息	132,297.27	流量检测与管理、网络入侵防范、下一代防火墙、主机入侵防御等 49 个领域	主要客户包括政府、金融企业、教育机构、电信运营商等
安博通	26,283.57	流量检测与管理、上网行为管理、下一代防火墙、威胁检测与响应、运营类态势感知 5 个领域	主要客户为产品和解决方案厂商
山石网科	72,538.88	通信安全、流量检测与管理、网络入侵防范、下一代防火墙等 23 个领域	金融、电信运营商、政府、互联网企业、教育等行业客户
奇安信	416,117.41	通信安全、流量检测与管理、上网行为管理、网络隔离等 85 个领域	集中在政府、公检法司、军队军工、能源、金融、教育机构、医疗卫生、电信运营商等行业单位
发行人	29,164.20	靶场和实验室、欺骗式防御、安全培训服务、渗透测试/众测、攻	主要客户为监管部门、关键信息基础设施单位等政企

		防演练、监管类态势感知、应急响应服务、重保服务 8 个领域	客户
--	--	-------------------------------	----

和同行业上市公司相比，公司规模较小，如奇安信、深信服、启明星辰、美亚柏科、绿盟科技等，收入均在 20 亿元以上。其涉及的网络安全行业领域较多，如奇安信涉及 85 个领域，深信服涉及 47 个领域，启明星辰涉及 55 个领域，绿盟科技涉及 62 个领域，而发行人共涉及 8 个领域，公司收入规模较小，涉及网络安全行业细分领域较少。

上市公司由于规模较大，网络安全领域较多，因此其客户一般涉及政府、电信、金融、能源等各个行业，客户行业丰富且一般采取直销和代销等多种销售渠道，而公司业务主要以项目制的形式体现。

和同行业规模较大的上市公司相比，公司规模较小，且未上市，公司的融资渠道匮乏，行业影响力低于部分同行业规模较大的上市公司。

公司已在招股说明书“第六节 业务和技术”之“二、发行人所处行业基本情况及其竞争状况”之“（四）发行人产品或服务的市场地位、技术水平及特点、行业内主要企业、竞争优势与劣势、行业发展态势、面临的机遇与挑战，以及报告期内的变化和趋势”之“5、公司竞争劣势”补充披露如下：

（1）公司产品种类较少

区别于传统安全产品公司，公司专注于网络靶场细分领域产品的研发、生产和销售，网络靶场具有较强的产品线延伸空间，但该领域尚处于起步阶段。和同行业规模较大的综合上市公司相比，目前公司产品种类较少，未覆盖如防火墙、IDS 以及安全审计类等市场占比较高的传统安全产品。

（2）公司处于业务成长期，业绩存在一定的波动性

公司目前处于业务快速成长期，专注于网络靶场细分领域核心技术研发及相关产品生产销售。公司主要以项目制形式开展业务，相比于已经形成市场规模的同行业上市公司，单体项目对公司业绩影响较大，业绩存在一定的波动性。

（3）公司融资渠道匮乏

公司作为一家以研发创新为驱动的企业，技术的不断创新和新产品的持续研发是公司不断发展的基础。为保持领先地位，公司需要不断进行技术的预研、产品的更新迭代、新产品的开发、高端人才的引进、以及新产品推广等，这些需要较大的资金投入。作为一家非上市企业，公司融资渠道相对匮乏，与同行

业 A 股上市公司相比，存在一定发展劣势。

(4) 公司规模较小

和同行业上市公司相比，公司规模较小，如奇安信、深信服、启明星辰、美亚柏科、绿盟科技等，收入均在 20 亿元以上。公司亟需进一步扩大整体经营规模，以提高自身经营业绩、抗风险能力以及行业影响力。

二、技术先进性

由于国内网络靶场起步较晚，尚未公布较为权威的技术指标，同行业公司亦未详细披露相关网络靶场信息，公司的网络靶场具有以下技术特征：

公司网络靶场主要指标如下所示：

靶场相关能力	具体情况
支持的靶场类型	赛事演练靶场； 人才培养靶场； 智慧城市安全测试靶场； 案件线索追踪实战靶场； 业务模拟靶场； 人工智能攻防靶场； 复杂业务安全推演靶场； 综合场景应用靶场（涵盖科技馆、人才基地等）。
仿真及虚拟化能力	全自主研发的春秋云靶场专用管理平台； 支持 KVM、docker、VMware、Xen、QEMU 等多种类型的虚拟机导入，兼容 OpenStack 等云平台接口； 支持全虚拟机、容器虚拟化、数字仿真、模拟仿真、协议仿真、流量仿真六维融合仿真技术； 支持与终端设备、路由交换设备、网络设备等多种类型的实体设备结合构建隔离的软件定义隔离网络，并支持自动化部署脚本进行快速状态恢复； 支持基于流量、自动化脚本等进行业务或特定的行为仿真。
已公开验证过的最大节点部署规模	2020 年“网鼎杯”半决赛现场，单一场景 8000+全虚拟机节点
可支持的最大节点部署规模	百万级节点多集群联动
千级别节点实例化时间	分钟级
单虚拟机节点实例化时间	秒级
并发及接入能力	支持多种类型的靶场任务并发下发，所有任务数据及虚拟化场景严格隔离； 支持单任务或多任务统一动态导调，支持动态数据采集及实时效能评估； 每个任务均支持攻击测试、防御、监管、厂商、供应链、普通应用者等多种角色按不同权限接入场景实时互动； 支持个人终端、VPN 远程、靶场操作虚拟机等各类接入模式。
成功支持基于网络靶场的省部级以上竞赛及演习案	网鼎杯、强网杯、护网杯、全国信息安全竞赛、巅峰极客网络安全大赛、粤盾演习、DefCon 中国赛、黄鹤杯 RHG 人工智能

例	安全大赛等。
靶标资源	百万级中低交互节点集群靶标； 操作系统虚拟机靶标 1500+； 高交互靶标 5000+； CVE 漏洞验证靶标 1000+； 漏洞知识库 20 万+； 各类漏洞环境 10000+； 高交互仿真场景 800+； 行业及城市级仿真场景 100+。
多级靶场级联或与其他平台兼容性	支持春秋云境靶场多级级联； 标准数据接口支持与其他网络靶场或管理系统进行兼容。

公司在招股说明书补充披露如下：

（一）发行人的核心技术先进性

公司经过多年的研发和实践，形成了体系化的城市级网络仿真靶场的理论方法、设计模式、主要技术及平台组建，并以此构建了国内首个仿真城市级、综合了互联网及行业基础设施内网的大型靶场，并作为大型网络对抗演习和竞赛的支持平台得到应用。该网络靶场具有高逼真、大规模、对抗性等特点，对网络安全训练、攻防演习、网络安全教学、城市级网络仿真、网络设备和信息系统的测试及验证等提供了有效支撑。网络靶场平台支撑了中央网信办、公安部、教育部、工信部等部委和单位主办或指导的超过 320 场网络安全演练。

公司网络靶场下发多级子网的百级别全靶机场景实例化不超过 12 秒、平台稳定性达到了 99.99%、成功支撑 20,000 人同时在线演练、并发实验场景超 8,000 个等。具有百万级中低交互节点集群靶标、超过 5,000 个高交互靶标、超过 800 个攻防场景、超过 10,000 个漏洞环境、超过 2,000 个网络实验工具、实现万级别节点统一下发等。

公司的网络靶场系列产品致力于解决网络安全仿真测试环境缺失问题、网络安全实用型人才培养与评价问题及网络安全防御有效性提升问题。公司自主研发的“人才培养靶场”和“赛事演练靶场”解决了网络安全实用型人才培养与评价的难题；研发的“业务模拟仿真靶场”“复杂业务安全推演靶场”和“智慧城市安全测试靶场”解决了政企客户在网络装置原型设计、方案决策、研发测试、测评检验、复杂安全问题定位和推演等过程中网络安全仿真环境缺失的问题；研发的“案件线索追踪实战靶场”为相关用户提供了专业规范的工具库及具有特定属性的专有空间，为客户解决实际业务过程中多维数据整合、数据

分析、复盘推演、指挥调度等全过程管理问题；研发的“人工智能攻防靶场”，为人工智能相关技术在网络安全领域的突破融合和实践测试等提供了基础的试验床和数据集，为漏洞挖掘与利用、综合智能攻防等人工智能安全技术的发展及效能验证提供了平台和测试数据集，成为了人工智能技术在网络安全领域实践的有效基础设施。综合应用型网络靶场是网络靶场多种应用场景集成的综合形态，发行人基于公司多项关键技术及核心产品构建了虚拟网络仿真场景，结合提炼和总结的国内外重大网络安全事件、众多前沿安全技术及各领域主流网络安全产品等内容，融合沙盘建设技术、大数据展示技术、模型构建技术、人机交互技术、动画和视频技术等形成了多种形态的靶场模块。通过沉浸式和高交互的体验模式，满足各类用户利用网络靶场进行情景式安全教育、实战式人才培养和考核、主流安全产品体验、网络安全演习、重大网络安全事件演练复盘等需求。

2018年10月25日，中科合创（北京）科技成果评价中心（科技部有关部门批准成立的全国第一家第三方专业科技成果评价机构）组织院士、行业专家等对公司“城市网络靶场构建技术及应用”进行集中评定，认定“该项目达到国内领先水平”。公司作为第一完成人的“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获2019年度北京市科学技术奖（科学技术进步奖）一等奖。

请发行人说明：

（1）安全企业级培训服务市场的市场空间；

根据 IDC 发布的《2020 年下半年中国 IT 安全服务市场跟踪报告》，IT 安全教育培训包括企业级培训服务（包括安全意识培训、安全技能培训、大型赛事、安全靶场等服务）、教育认证（包括认证培训、认证考核）和高校教育组成，发行人在 2020 年企业级培训服务市场中占比 23.35%，排名第一，根据 IDC 调研，发行人相关数据为 3,300.20 万美元，占比 23.30%，因此 2020 年企业级培训服务市场为 14,249.79 万美元，约合人民币 10 亿元。公司连续 4 年在企业级培训服务市场排名第一，企业级培训服务市场总量由 2017 年的 47,973.39 万元增长到 2020 年的 98,283.83 万元，复合增长率为 27.01%，增长率较高。

IDC 在统计企业级培训服务时，将网络靶场统计在内，因此公司占比较高，

也间接说明了公司网络靶场的市场份额。

(2) 发行人在网络安全竞赛服务方面具有明显的领先地位的体现, 2018 年“城市网络靶场构建技术及应用”评定结果作为发行人技术达到国内领先水平的依据是否充分。

一、网络安全竞赛服务

在网络安全竞赛服务方面, 公司具有明显的领先地位, 公司成立至今, 成功支持或举办了超过 320 场大中型网络安全赛事, 参赛人次超过 38 万, 为中央网信办、公安部、工信部、卫健委、教育部、科技部、国家税务总局等国家部委及全国十余个行业通过设计高水平网络安全赛事服务形成人才训练、评价、选拔机制, 打造了网鼎杯、强网杯、巅峰极客、护网杯、RHG 等网络安全赛事高峰。公司通过专业的赛事运营服务形成了具有影响力的网络安全赛事品牌——“春秋 GAME”, 推动网络安全赛事运动在中国的蓬勃发展。

(一) 从比赛规格上来看

从比赛规格上来看, 主要国家级的网络安全比赛都有发行人的参与, 如连续两届支持了公安部主导 2018 年开始的两年一届的“网鼎杯”、支持了 2018 年、2020 年、2021 年中央网信办指导的一年一届“强网杯”、工信部主办的“全国工业互联网安全技术技能大赛”、信息安全重点实验室主办的“RHG 机器人网络安全大赛”、聚焦数字安全防护的国家级赛事“陇剑杯”网络安全大赛等一系列重大的网络安全赛事和演练活动, 在网络安全市场建立了良好的口碑。

(二) 从比赛规模上来看

由公安部主导的“网鼎杯”是国内影响力最大的网络安全比赛之一, 2018 年首届“网鼎杯”, 7,000 多支队伍、2.25 万人参赛, 创造了最大规模网络安全赛事纪录, 2020 年第二届“网鼎杯”共有 14,724 支战队, 39,613 人参加, 大赛规模再次打破记录。

第一届“网鼎杯”由发行人主办, 阿里巴巴、百度、腾讯、360、中国科学院、清华大学联合协办, 第二届“网鼎杯”由发行人和深信服联合主办, 由阿里巴巴、百度、腾讯、中国科学院、奇安信、清华大学联合协办。两届“网鼎杯”均由发行人参与主办且由发行人提供技术支持, 由阿里巴巴、百度、腾讯、360、奇安信等知名互联网公司或网络安全公司协办, 清华大学、中国科学院等顶级院

校协办，足以体现了社会对发行人技术能力的认可、承办比赛能力的认可。

（三）从技术上来看

从技术上来看，目前网络安全赛事赛制常见的有 CTF（夺旗赛）、AWD（攻防兼备）、靶场赛、理论题等，较为不常见的主要有 KOH（车轮赛）、RHG（人工智能大赛）、运维大师赛、工控攻防大赛、取证赛等等，公司能够支持各工种赛制。各种赛制中 AWD、RHG、城市靶场赛、运维大师赛等国内第一场比赛都是由公司举办或支持。

支持赛事的底层技术，“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获 2019 年度北京市科学技术奖（科学技术进步奖）一等奖，公司董事长蔡晶晶被中央网信办评为“网络安全优秀人才”。

二、网络靶场处于国内领先地位的依据

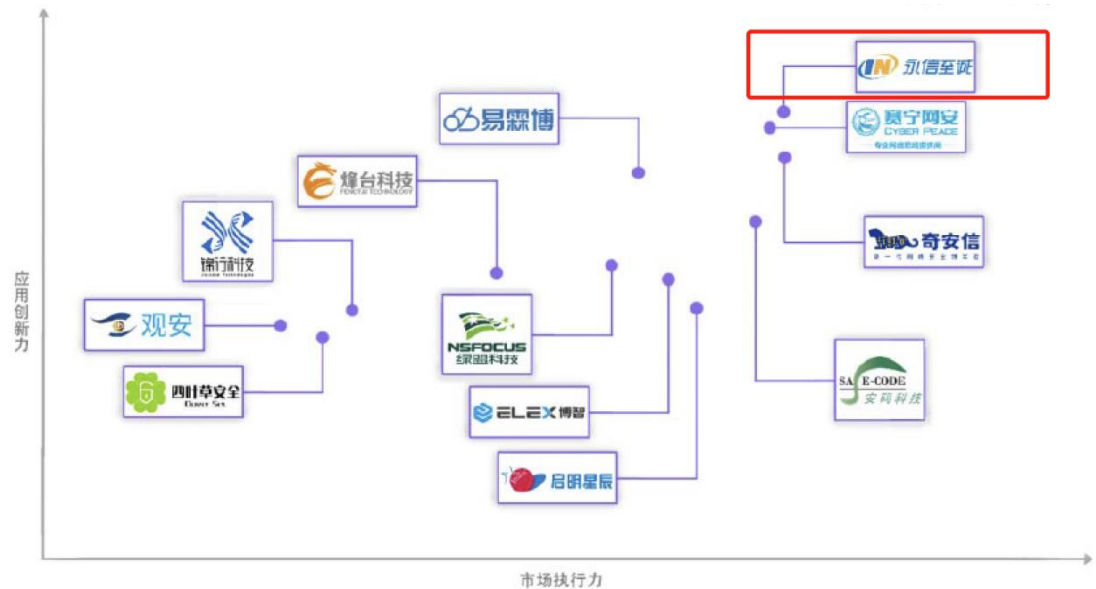
公司经过连续七年的持续迭代和运营，公司春秋云境网络靶场已覆盖教育、通信、交通、国防工业、能源、金融、政法、电子政务、科技、互联网等十余个行业，积累了数百个行业级场景，近百个城市级仿真互联网场景，近千个网络安全 CVE 漏洞靶标，数千个安全实训靶标，百余个人工智能漏洞挖掘训练集等。2020 年 11 月，公司成功构建了城市级网络靶场“网鼎之城”，该靶场包含超过 8,000 个计算节点和 1,200 余个虚实结合的业务场景，支持了近两千人同场演练。公司靶场技术已达到国内领先水平，主要依据如下：

序号	内容	认定机构
1	2018 年 10 月 25 日，中科合创（北京）科技成果评价中心组织院士等专家对公司的“城市网络靶场构建技术及应用”进行集中评定，认定“该项目达到国内领先水平”。	中科合创（北京）科技成果评价中心，具有中国科技部颁发的科学技术成果评价试点机构证书。
2	基于平行仿真的大规模网络靶场构建技术及应用项目荣获 2019 年度北京市科学技术奖（科学技术进步奖）一等奖	北京市人民政府
3	2018 年网络安全创新产品（技术）一等奖-网络安全实验室靶场平台	国家计算机网络应急技术处理协调中心
4	数世咨询发布《网络靶场能力指南》，公司网络靶场应用创新力和市场执行力均第一。	国内数字领域第三方调研机构数世咨询（北京数字世界咨询有限公司）

公司网络安全实验室靶场平台荣获了 2018 年网络安全产品（技术）一等奖；并且在 2018 年 10 月 25 日，经过了中科合创（北京）科技成果评价中心（科技部有关部门批准成立的全国第一家第三方专业科技成果评价机构）组织院士等专

家对公司的“城市网络靶场构建技术及应用”进行集中评定，认定“该项目达到国内领先水平”；2019 年公司基于平行仿真的大规模网络靶场构建技术及应用项目荣获了 2019 年度北京市科学技术奖（科学技术进步奖）一等奖。

2020 年国内数字领域第三方调研机构数世咨询发布了《网络靶场能力指南》，数世咨询将网络靶场定义为新兴市场，入选的安全厂家有 12 家，公司网络靶场应用创新力和市场执行力均第一，具体如下所示：



【保荐机构核查程序】

- 1、访谈发行人核心技术人员，了解发行人技术先进性的主要体现；
- 2、通过网络公开信息查询同行业可比上市公司的产品情况和经营规模，分析发行人竞争优势和竞争劣势；
- 3、获取行业研究报告，查询网络公开信息，了解发行人所处细分领域的市场空间；
- 4、访谈发行人总经理，了解发行人在网络安全竞赛服务方面的市场份额；
- 5、查阅行业研究报告，获取发行人主要奖项及认证清单，了解发行人的市场地位。

【保荐机构核查意见】

- 经核查，保荐机构认为：
- 1、发行人在网络靶场领域具有技术先进性，但相关标准尚无法与同行业可比公司直接对比；

2、发行人在细分行业具有技术先进性，同时也存在产品种类较少、业绩存在一定的波动性等竞争劣势；

3、发行人在网络安全竞赛服务方面具有明显的领先地位；网络靶场处于国内领先地位经由权威机构认证。

5、关于业务资质

根据申报材料：（1）发行人涉密信息系统集成资质证书为公司从事国安、公安等涉密业务所需的资质，该资质已于 2020 年 12 月到期，公司已于 2020 年 11 月重新提出资质申请。根据《涉密信息系统集成资质管理办法》规定，有效期满且申请未经保密行政管理部门准予许可前，不得签订新的涉密信息系统集成业务合同；（2）发行人线上网络安全实训载体为 i 春秋网站，该等网站设置有视频课程版块，发行人暂未取得《信息网络传播视听节目许可证》，但仍不排除未来可能由于因行业监管政策变化或有权机关明确要求等因素，导致发行人继续从事目前开展的业务需办理上述资质证书；（3）除“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0 APT 安全监测产品（增强级）”产品外，发行人其他产品均未办理《计算机信息系统安全专用产品销售许可证》；（4）发行人业务存在跨区情形但没有申请《增值电信业务经营许可证（IDC 业务）》全国性证书。

请发行人说明：（1）涉密信息系统集成资质证书目前的续展进展，无法取得上述证书的可能性；（2）公司目前开展网络培训业务无需获得《信息网络传播视听节目许可证》是否符合《网络安全法》《网络音视频信息服务管理规定》等相关规定，结合报告期内的相关业务的收入金额、占比及未来发展规划情况等，量化分析如果未来需要取得上述资质才能开展相关培训业务对公司持续经营的影响；（3）除“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0 APT 安全监测产品（增强级）”产品外，发行人其他产品均无需办理《计算机信息系统安全专用产品销售许可证》的依据，是否符合相关法规要求和行业惯例；（4）结合发行人的业务开展地域情况，说明是否存在超出《增值电信业务经营许可证（IDC 业务）》范围进行经营的情形；（5）结合具体业务类型及相关法律法规，说明相关业务开展过程中是否需要取得计算机信息系统集成资质、军用信息安全产品认证证书、涉密信息系统产品检测证书、信息安全服务资质证书等。

请保荐机构、发行人律师对上述事项以及发行人是否存在未取得相应资质即

进行经营事项进行核查，发表明确意见。

【回复】

发行人说明：

(1) 涉密信息系统集成资质证书目前的续展进展，无法取得上述证书的可能性；

截至本回复出具之日，发行人已取得了续展后的《涉密信息系统集成资质甲级-软件开发》资质证书，证书有效期为 2021 年 9 月 23 日至 2026 年 9 月 22 日。

根据《涉密信息系统集成资质管理办法》第二十八条的规定，涉密信息系统集成资质证书有效期届满且未准予延续前，不得签订新的与《涉密信息系统集成资质甲级-软件开发》资质相关的业务合同。对于已经签订合同但未完成的涉密业务，在确保安全保密的条件下可以继续完成。

公司按照上述规定，在完成《涉密信息系统集成资质甲级-软件开发》资质的续展前，发行人并未签订新的与《涉密信息系统集成资质甲级-软件开发》资质相关的业务合同。

综上，发行人已取得了续展后的《涉密信息系统集成资质甲级-软件开发》资质证书，并且在完成《涉密信息系统集成资质甲级-软件开发》资质的续展前，发行人并未签订新的与《涉密信息系统集成资质甲级-软件开发》资质相关的业务合同。发行人不存在无法续展《涉密信息系统集成资质甲级-软件开发》资质而对发行人的业务产生重大不利影响的情形。

(2) 公司目前开展网络培训业务无需获得《信息网络传播视听节目许可证》是否符合《网络安全法》《网络音视频信息服务管理规定》等相关规定，结合报告期内的相关业务的收入金额、占比及未来发展规划情况等，量化分析如果未来需要取得上述资质才能开展相关培训业务对公司持续经营的影响；

一、发行人无需获得《信息网络传播视听节目许可证》符合《网络安全法》《网络音视频信息服务管理规定》等相关规定

《网络安全法》未就开展网络培训业务所需的资质进行明确规定，但其第九条规定，“网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。”《网络音视频信息服务管理规定》第六条规定，“网络

音视频信息服务提供者应当依法取得法律、行政法规规定的相关资质”。

根据《互联网视听节目服务管理规定》第七条规定，从事互联网视听节目服务的，需要取得广播电影电视主管部门颁发的《信息网络传播视听节目许可证》或履行备案手续。

北京市广播电视局在其官方网站答复：“国家广播电视总局相关通知明确指出：互联网教育企业开展以提高特定人群专业水平为目的的网络视音频教学活动，如通过互联网开展学前教育、基础教育、高等教育、职业教育等的远程教育活动不属于《互联网视听节目服务管理规定》管理范畴。”

发行人开展的网络培训业务是以提高特定人群专业水平为目的的教育活动，不属于《互联网视听节目服务管理规定》管理范畴，因此无需取得《信息网络传播视听节目许可证》。

此外，根据北京市文化市场综合执法总队于 2021 年 9 月 10 日出具的《行政处罚查询告知书》，发行人自 2018 年 1 月 1 日至 2021 年 7 月 31 日，没有因违反文化方面行政管理相关法律法规受到该单位或住所地文化和旅游局行政处罚的记录。

综上，发行人开展网络培训业务无需获得《信息网络传播视听节目许可证》不违反《网络安全法》《网络音视频信息服务管理规定》等相关规定。

二、如需取得《信息网络传播视听节目许可证》才能开展相关培训业务对公司持续经营的影响

报告期内发行人线上安全培训收入金额及占比如下：

单位：万元

分类	2021 年 1-6 月	2020 年	2019 年	2018 年
线上安全培训收入	50.95	284.74	214.99	137.22
营业收入总额	8,136.08	29,164.20	16,308.54	18,051.03
占比	0.63%	0.98%	1.32%	0.76%

因此，网络培训业务占发行人营业收入比重较小，同时网络培训业务在发行人的未来规划中不属于核心业务方向，如需取得《信息网络传播视听节目许可证》才能开展相关培训业务，不会对发行人业务的持续经营产生重大不利影响。

如未来因行业监管政策变化或有权机关明确要求等因素导致发行人继续从事目前开展的业务需办理《信息网络传播视听节目许可证》资质证书的，发行人

将考虑采取将相关视频上传、存储至有资质的第三方网络平台等方式开展相关业务。

(3) 除“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0APT 安全监测产品（增强级）”产品外，发行人其他产品均无需办理《计算机信息系统安全专用产品销售许可证》的依据，是否符合相关法规要求和行业惯例；

目前，除已取得的《计算机信息系统安全专用产品销售许可证》外，发行人其他产品因不属于用于保护计算机系统安全的专用硬件或软件产品，亦不属于“公安部计算机信息系统安全专用产品销售许可服务平台”列示的“标准和规范列表”范围内，因此无需办理《计算机信息系统安全专用产品销售许可证》。

一、发行人已取得 3 个《计算机信息系统安全专用产品销售许可证》

计算机信息系统安全专用产品实行销售许可证制度，该等产品的生产者在该产品进入市场销售之前，必须申领《计算机信息系统安全专用产品销售许可证》。除“春秋云阵蜜罐系统”“慧眼高级威胁检测系统 V2.0APT 安全监测产品（增强级）”产品外，发行人还于 2021 年 7 月 8 日取得了“安全可视化日志分析平台 ECQ-TSGZ-A100/V1.0 日志分析（一级）”的《计算机信息系统安全专用产品销售许可证》。随着发行人的产品研发和业务发展需要，发行人将根据实际情况申请办理新的《计算机信息系统安全专用产品销售许可证》。

发行人已取得 3 个《计算机信息系统安全专用产品销售许可证》，具体情况如下：

序号	公司名称	资质/许可	证书编号	产品名称	核发部门	有效期限
1	发行人	计算机信息系统安全专用产品销售许可证	0503201087	计算机信息系统安全专用产品销售许可证-春秋云阵蜜罐系统 ECQYZ-HA/V2.0 主机型入侵检测产品（基本级）	公安部网络安全保卫局	2020.8.8 - 2022.8.8
2	发行人	计算机信息系统安全专用产品销售许可证	0108201163	计算机信息系统安全专用产品销售许可证-慧眼高级威胁检测系统 S1-V2.0 APT	公安部网络安全保卫局	2020.8.15 - 2022.8.15

序号	公司名称	资质/许可	证书编号	产品名称	核发部门	有效期限
				安全监测产品（增强级）		
3	发行人	计算机信息系统安全专用产品销售许可证	0405211221	计算机信息系统安全专用产品销售许可证-安全可视化日志分析平台 ECQ-TSGZ-A100/V1.0 日志分析（一级）	公安部网络安全保卫局	2021.7.8 - 2023.7.8

二、《计算机信息系统安全专用产品销售许可证》的适用范围

（一）计算机信息系统安全专用产品的范围

根据《计算机信息系统安全保护条例》《计算机信息系统安全专用产品检测和销售许可证管理办法》以及“公安部计算机信息系统安全专用产品销售许可服务平台”列示的“标准和规范列表”，目前纳入“标准和规范列表”的适用产品类型共 94 类，且该等 94 类产品均为用于保护计算机系统安全的专用硬件或软件产品。经咨询公安部网络安全保卫局，未在“标准和规范列表”范围内的网络安全产品，无法申请办理《计算机信息系统安全专用产品销售许可证》。

（二）发行人的产品是否属于计算机信息系统安全专用产品

目前，发行人的主要产品包括网络靶场系列产品、安全管控与蜜罐产品和安全工具类产品，其中网络靶场系列产品不属于“公安部计算机信息系统安全专用产品销售许可服务平台”列示的“标准和规范列表”中的计算机信息系统安全专用产品，安全管控与蜜罐产品和安全工具类产品中的部分产品属于计算机信息系统安全专用产品。具体如下：

产品分类（一级）	产品分类（二级）	是否获得销售许可证	未获得销售许可证的原因
网络靶场系列产品	春秋云境网络靶场平台	否	未纳入销售许可证“标准和规范列表”
安全管控与蜜罐产品	春秋云阵新一代蜜罐系统	是	-
	春秋云势网络安全态势感知与处置平台	否	未纳入销售许可证“标准和规范列表”
安全工具类产品	流量监测类产品	慧眼高级威胁检测系统已获得销售许可证	除已取得《计算机信息系统安全专用产品销售许可证》的产品外，其余产品未纳入销售许可证“标准和规范

			列表”
	数据分析类产品	安全可视化日志分析平台已获得销售许可证	除已取得《计算机信息系统安全专用产品销售许可证》的产品外，其余产品未纳入销售许可证“标准和规范列表”
	业务支撑类产品	否	未纳入销售许可证“标准和规范列表”
	安全辅助类产品	否	未纳入销售许可证“标准和规范列表”

1、网络靶场系列产品

“公安部计算机信息系统安全专用产品销售许可服务平台”所列示的“标准和规范列表”未包含网络靶场系列产品，因此网络靶场系列产品无需办理《计算机信息系统安全专用产品销售许可证》。

2、安全管控与蜜罐产品

安全管控与蜜罐产品主要包括春秋云阵新一代蜜罐系统和春秋云势网络安全态势感知与处置平台。

（1）春秋云阵新一代蜜罐系统

蜜罐产品属于“标准和规范列表”列示的“主机型入侵检测产品”，应当取得《计算机信息系统安全专用产品销售许可证》。发行人的蜜罐产品春秋云阵新一代蜜罐系统已通过检测，并获得春秋云阵蜜罐系统 ECQYZ-HA/V2.0 主机型入侵检测产品（基本级）《计算机信息系统安全专用产品销售许可证》。

（2）春秋云势网络安全态势感知与处置平台

春秋云势网络安全态势感知与处置平台是根据客户需求专门定制的一体化产品。作为一体化产品的春秋云势网络安全态势感知与处置平台非基础技术模块的简单拼接，而是集自主研发软件、第三方采购硬件、支持性服务为一体化的综合性产品。“公安部计算机信息系统安全专用产品销售许可服务平台”所列示的“标准和规范列表”并未包含作为一体化产品的春秋云势网络安全态势感知与处置平台，因此，春秋云势网络安全态势感知与处置平台无需办理《计算机信息系统安全专用产品销售许可证》。

尽管春秋云势网络安全态势感知与处置平台不需要获得《计算机信息系统安全专用产品销售许可证》，但如对其技术方案中包含基础技术模块进一步开发，

使之成为独立的产品，则应比照“公安部计算机信息系统安全专用产品销售许可服务平台”所列示的“标准和规范列表”申请办理《计算机信息系统安全专用产品销售许可证》。目前，基于春秋云势网络安全态势感知与处置平台进一步开发的“慧眼高级威胁检测系统”和“安全可视化日志分析平台”已形成独立的产品，并取得了《计算机信息系统安全专用产品销售许可证》，该两项产品已作为安全工具类产品进行销售。

3、安全工具类产品

安全工具类产品包括流量监测类产品、数据分析类产品、业务支撑类产品和安全辅助类产品。其中流量监测类产品是针对流量数据进行捕获分析和监测预警的系列产品；数据分析类产品是指利用大数据分析技术，通过预先设定的事件处理拓扑，快速搭建事件处理流程；业务支撑类产品是针对国家监管部门日常综合性管理需求定制开发的产品；安全辅助类产品是针对国家监管部门信息采集、网络调查、业务分析、网络取证定制开发的产品。

对于属于“公安部计算机信息系统安全专用产品销售许可服务平台”所列示的“标准和规范列表”范围的计算机系统专用安全软硬件产品，发行人均已取得《计算机信息系统安全专用产品销售许可证》，包括流量监测类产品中的“慧眼高级威胁检测系统”和数据分析类产品中的“安全可视化日志分析平台”。慧眼高级威胁检测系统属于“标准和规范列表”中的“APT 安全监测产品”，安全可视化日志分析平台属于“标准和规范列表”中的“日志分析产品”。

发行人的其他安全工具类产品，由于不属于“公安部计算机信息系统安全专用产品销售许可服务平台”所列示的“标准和规范列表”范围，因此无需办理《计算机信息系统安全专用产品销售许可证》。

除已获得《计算机信息系统安全专用产品销售许可证》的产品外，报告期内发行人其他产品均无需办理《计算机信息系统安全专用产品销售许可证》符合相关法规要求和行业惯例。

（4）结合发行人的业务开展地域情况，说明是否存在超出《增值电信业务经营许可证（IDC 业务）》范围进行经营的情形；

发行人已开展的业务不涉及 IDC 业务，不存在业务开展地域超出《增值电信业务经营许可证（IDC 业务）》范围进行经营的情形。

一、发行人已开展的业务不涉及互联网数据中心（IDC）业务

根据《电信业务经营许可管理办法》《电信业务分类目录》相关规定，互联网数据中心（IDC）业务是指利用相应的机房设施，以外包出租的方式为用户的服务器等互联网或其他网络相关设备提供放置、代理维护、系统配置及管理服务，以及提供数据库系统或服务器等设备的出租及其存储空间的出租、通信线路和出口带宽的代理租用和其他应用服务。

发行人在销售网络靶场系列产品、安全管控与蜜罐等产品过程中，会基于客户的服务器、带宽使用需求，从服务商租赁服务器和带宽，作为所销售产品的配套，整体交付给客户使用。发行人在上述产品开发模式中，不存在利用相应的机房设施以外包出租的方式为客户提供服务器和带宽等服务的情形，因此不属于 IDC 业务。

二、发行人已取得《增值电信业务经营许可证》，但尚未开展 IDC 业务

发行人于 2021 年 4 月 21 日取得《增值电信业务经营许可证》（证书编号“B1-20211408”），业务种类为互联网数据中心业务，机房所在地为北京、福州、广州。由于国家对电信业务经营实行许可制度，发行人在取得该《增值电信业务经营许可证》后即有权开展 IDC 业务。发行人承诺，如后续开展 IDC 业务，将在所取得《增值电信业务经营许可证》的许可范围内开展。

三、发行人开展有关业务的合法合规性

经检索国家企业信用信息公示系统、北京市市场监督管理局、北京市经济和信息化局等公示信息，发行人不存在因违反法律规定超出资质规定范围开展业务而受到行政处罚的记录。

综上，发行人已开展的业务不涉及 IDC 业务，不存在超出《增值电信业务经营许可证（IDC 业务）》范围进行经营的情形。

（5）结合具体业务类型及相关法律法规，说明相关业务开展过程中是否需要取得计算机信息系统集成资质、军用信息安全产品认证证书、涉密信息系统产品检测证书、信息安全服务资质证书等。

1、计算机信息系统集成资质

计算机信息系统集成资质已被废止。

1999 年 12 月 7 日，信息产业部发布的《计算机信息系统集成资质管理办法

（试行）》第四条规定“凡从事计算机信息系统集成业务的单位，必须经过资质认证并取得了《计算机信息系统集成资质证书》”。

2016年6月2日，工业和信息化部发布的2016年第26号公告将《计算机信息系统集成资质管理办法（试行）》废止。

2018年12月29日，工业和信息化部发布《关于计算机信息系统集成行业管理有关事项的通告》（工信部信软函〔2018〕507号），明确“计算机信息系统集成企业资质认定”已于2014年由国务院明令取消，任何组织和机构不得继续实施。

因此，发行人开展的业务无需办理计算机信息系统集成资质。

2、军用信息安全产品认证证书

军用信息安全产品认证证书由中国人民解放军信息安全测评认证中心颁发。

根据《中国人民解放军计算机信息系统安全保密规定》第二十九条的规定，用于军队计算机信息系统安全保密防护与检测的硬件、软件和系统，必须选用军内或者国内研制开发并经解放军信息安全测评认证中心测评认证的产品。

报告期内，发行人不存在向军队客户销售用于军队计算机信息系统安全保密防护与检测的硬件、软件和系统的情形。

因此，发行人开展的业务无需办理《军用信息安全产品认证证书》。

3、涉密信息系统产品检测证书

《涉密信息系统产品检测证书》由国家保密科技测评中心颁发。由该中心检测并颁发涉密信息系统产品检测证书的产品包括：安全保密产品、安全隔离与信息单向导入系统产品，和屏蔽机柜、传导干扰器等电磁泄露发射防护产品等。

由该中心检测并颁发的《涉密信息系统产品检测证书》并非一项行政许可，不是法律强制要求的准入型资质，而是属于自愿性的产品认证，且发行人未销售上述产品，因此发行人无需办理《涉密信息系统产品检测证书》。

4、信息安全服务资质证书

《信息安全服务资质证书》是由中国网络安全审查技术与认证中心进行认证。该中心检测并颁发的《信息安全服务资质证书》并非一项行政许可，不是法律强制要求的准入型资质，而是属于自愿性的产品认证。

根据上海证券交易所科创板上市公司北京安博通科技股份有限公司于 2019 年 5 月 6 日披露的《关于北京安博通科技股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复》，“信息安全服务资质认证等非强制性认证工作，公司及其子公司已根据其自身业务发展需要取得相关认证。”

因此，发行人未取得《信息安全服务资质证书》并不违反法律、行政法规的规定。

报告期内，发行人根据自身业务发展需要，取得了如下 4 项《信息安全服务资质证书》：

序号	公司名称	资质名称	证书编号	核发部门	有效期限
1	发行人	信息安全服务资质认证证书（信息安全应急处理服务资质三级）	CCRC-2018-ISV-ER-203	中国网络安全审查技术与认证中心	2018.10.17 - 2022.1.16
2	发行人	信息安全服务资质认证证书（信息安全风险评估服务资质三级）	CCRC-2018-ISV-RA-455	中国网络安全审查技术与认证中心	2018.10.17 - 2022.1.16
3	发行人	信息安全服务资质认证证书（信息系统安全运维服务资质三级）	CCRC-2018-ISV-SM-315	中国网络安全审查技术与认证中心	2018.10.17 - 2022.1.16
4	发行人	信息安全服务资质认证证书（信息系统安全集成服务资质三级）	CCRC-2018-ISV-SI-1004	中国网络安全审查技术与认证中心	2018.10.17 - 2022.1.16

（6）发行人是否存在未取得相应资质即进行经营事项

发行人的主营业务为网络安全产品的研发、生产和销售，以及为客户提供网络安全服务。除已取得相关资质的业务外，发行人的业务不存在需要取得相应资质方可进行经营的事项。发行人已取得开展业务所需的资质，不存在未取得相应资质即进行经营的情况。

【核查程序】

1、取得发行人报告期内与涉密信息系统集成资质相关的销售合同，并查阅了发行人续展后的《涉密信息系统集成资质甲级-软件开发》资质证书；

2、电话咨询北京市广播电视局了解需办理《信息网络传播视听节目许可证》的业务范围，并查询北京市广播电视局网站关于《信息网络传播视听节目许可证》

的有关答复；

3、取得发行人报告期内的主营业务收入明细，了解报告期内发行人线上安全培训收入情况；

4、访谈发行人负责人及子公司五一嘉峪负责人，了解发行人对网络培训业务的规划；

5、登录“公安部计算机信息系统安全专用产品销售许可服务平台”，查询发行人已取得的《计算机信息系统安全专用产品销售许可证》；

6、取得发行人报告期内的销售合同，访谈发行人研发人员和业务人员，了解所销售产品的功能，将销售产品与“公安部计算机信息系统安全专用产品销售许可服务平台”列示的“标准和规范列表”进行比对；

7、电话咨询国家保密科技测评中心和中国网络安全审查技术与认证中心，分别就《涉密信息系统产品检测证书》和《信息安全服务资质证书》的性质进行确认；

8、访谈发行人负责人，全面了解发行人的业务开展情况，检索法律法规并就发行人已取得的资质与监管规范进行逐一比对。

【核查意见】

经核查，保荐机构及发行人律师认为：

1、发行人已取得了续展后的《涉密信息系统集成资质甲级-软件开发》资质证书，并且在完成《涉密信息系统集成资质甲级-软件开发》资质的续展前，发行人并未签订新的与《涉密信息系统集成资质甲级-软件开发》资质相关的业务合同。发行人不存在无法续展《涉密信息系统集成资质甲级-软件开发》资质而对发行人的业务产生重大不利影响的情形；

2、发行人开展网络培训业务无需取得《信息网络传播视听节目许可证》符合相关法律、法规规定。网络培训业务占发行人营业收入比重较小，如需取得《信息网络传播视听节目许可证》才能开展相关培训业务，不会对发行人业务的持续经营产生重大不利影响；

3、除已获得《计算机信息系统安全专用产品销售许可证》的产品外，报告期内发行人其他产品均无需办理《计算机信息系统安全专用产品销售许可证》符合相关法规要求和行业惯例；

4、发行人已开展的业务不属于互联网数据中心（IDC）业务，不存在超出《增值电信业务经营许可证（IDC 业务）》范围进行经营的情形；

5、发行人无须取得《计算机信息系统集成资质》《军用信息安全产品认证证书》《涉密信息系统产品检测证书》，《信息安全服务资质证书》属于自愿性产品认证，发行人已根据业务需要取得 4 项证书。

6、发行人不存在未取得相应资质即进行经营的情况。

6、关于采购和供应商

根据申报材料：（1）公司对外采购包括硬件设备、软件及技术服务，硬件设备为产品生产所需要的服务器、计算机；（2）报告期各期采购软件及技术服务金额分别为 2,086.63 万元、3,135.47 万元和 7,569.10 万元；硬件设备金额分别为 1,691.81 万元、1,133.01 万元和 2,175.46 万元；（3）定制化的靶场实验室平台建设以及“网络安全科技馆”项目需要一部分装修工程及非核心技术能力的技术采购。

请发行人补充披露：向前五大供应商采购的具体内容。

请发行人说明：（1）剔除“网络安全科技馆”项目影响后硬件设备、软件及技术服务的采购金额及变动原因；（2）软件及技术服务的具体内容及在发行人产品/服务中的应用情况、主要供应商情况；（3）靶场实验室平台建设需采购装修工程的原因及采购金额，服务的提供方。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见。

【回复】

请发行人补充披露：

（1）向前五大供应商采购的具体内容。

发行人已按要求在《招股说明书》“第六节 业务和技术”之“四、发行人采购情况和主要供应商”之“（二）主要供应商情况”对相关情况进行了补充披露，具体如下：

2021 年 1-6 月前五大供应商及采购的具体内容如下：

单位：万元

序号	供应商名称	采购金额	占年度采购总额的比例	采购内容
----	-------	------	------------	------

1	北京银达兴业建筑工程公司	388.29	9.72%	建筑装饰
2	北京数信网安科技有限公司	228.40	5.72%	硬盘、服务器等
3	奇安信科技集团股份有限公司	164.56	4.12%	安全检测与风险评估服务等
4	公安部第一研究所	141.51	3.54%	信息暴露检测、渗透测试服务等
5	北京神州泰岳软件股份有限公司	130.19	3.26%	专项技术培训、漏洞测试及驻场服务等
	总计	1,052.95	26.35%	-

2020 年前五大供应商及采购的具体内容如下：

单位：万元

序号	供应商名称	采购金额	占年度采购总额的比例	采购内容
1	随锐科技集团股份有限公司	589.62	5.64%	科技馆意识闯关、安全射击等趣味游戏模块开发
2	北京数信网安科技有限公司	506.81	4.85%	硬盘、网卡、服务器等
3	北京鹏途腾飞科技有限公司	367.92	3.52%	动画视频制作及剪辑
4	北京中顺诚科技有限公司	358.49	3.43%	动画影片制作
5	北京百度网讯科技有限公司	331.49	3.17%	科技馆 AI 手势识别、AI 图片识别等部分展项的制作
	总计	2,154.33	20.60%	-

2019 年前五大供应商及采购的具体内容如下：

单位：万元

序号	供应商名称	采购金额	占年度采购总额的比例	采购内容
1	北京数信网安科技有限公司	440.21	9.18%	硬盘、服务器等
2	北京明略软件系统有限公司	337.74	7.05%	安全防护软件开发技术
3	随锐科技集团股份有限公司	311.32	6.49%	应用漏洞发现及利用服务
4	西安长峰机电研究所	246.90	5.15%	大数据实时存储及计算系统
5	上海术推科技服务事务所	203.94	4.25%	VPS、技术支持服务
	总计	1,540.12	32.13%	-

2018 年前五大供应商及采购的具体内容如下：

单位：万元

序号	供应商名称	采购金额	占年度采购总额的比例	采购内容
----	-------	------	------------	------

			比例	
1	北京英信未来科技有限公司	521.24	12.71%	硬盘、服务器等
2	上海术推科技服务事务所	343.01	8.36%	VPS、技术支持服务等
3	安徽云探索网络科技有限公司	316.88	7.73%	系统开发、技术维护及数据资源服务
4	深圳零天科技有限公司	141.51	3.45%	技术服务
5	新疆汇鑫嘉业建筑装饰工程有限责任公司	118.89	2.90%	房屋建筑装修施工
	总计	1,441.53	35.15%	-

请发行人说明：

(1) 剔除“网络安全科技馆”项目影响后硬件设备、软件及技术服务的采购金额及变动原因；

报告期内，公司采购软件及技术服务金额分别为 2,086.63 万元、3,135.47 万元、7,569.10 万元和 2,527.03 万元，硬件设备金额分别为 1,691.81 万元、1,133.01 万元、2,175.46 万元和 756.67 万元，剔除“网络安全科技馆”项目影响后的变动情况如下：

单位：万元

类别	2021 年 1-6 月	2020 年（剔除后）	2019 年	2018 年
软件及技术服务	2,527.03	3,189.45	3,135.47	2,086.63
硬件设备	756.67	1,497.42	1,133.01	1,691.81
其他	712.68	110.34	525.17	323.17
合计	3,996.38	4,797.21	4,793.65	4,101.59

剔除“网络安全科技馆”项目采购后，报告期内公司三类采购金额基本保持稳定，其中其他类采购主要指建筑工程采购。2019 年和 2020 年软件及技术服务采购有较大幅度增长，主要由于公司对网络安全产品业务中客户所需求的部分用于加密传输、数据存储管理的成品系统直接进行了外采；同时针对安全工具类产品及安全防护系列服务所需的漏洞发现软件开发、评估渗透服务等，出于业务需要，公司进行了技术外采。2019 年公司硬件设备采购有所下降，主要因为 2019 年公司网络安全产品销售收入下降，因此导致发生硬件采购减少。2020 年公司其他类采购下降原因系靶场实验室平台建设项目所需的装修建筑类采购有所下降所致。

(2) 软件及技术服务的具体内容及在发行人产品/服务中的应用情况、主要

供应商情况；

一、软件及技术服务的具体内容及在发行人产品/服务中的应用情况

公司所采购的软件及技术服务主要包括基础设施、网络环境等业务必须的支持性采购，安全服务类采购，成品系统及系统开发采购，外包和培训、运维服务等其他采购 5 类，具体采购内容及在产品和服务中的应用如下表所示：

序号	采购类型	主要采购内容	在公司产品/服务中的应用
1	基础设施、网络环境等业务必须的支持性采购	VPS、云服务器租赁等网络环境采购及现场布展、场地租赁等支持性采购	为公司的各项产品及服务提供基础设施及支持性服务的采购。
2	安全服务类采购	漏洞测试分析、风险评估、安全检测与支撑服务等	出于公司资源等原因，公司对客户合同中的部分需求，如网络流量管理、数据清洗、安全体系建设的支撑等进行了外采，以保证在合同约定日期内完成对相关产品和服务的交付使用。
3	成品系统及系统开发采购	主要用于安全、办公、测评、展示、培训及存储等成品软件及定制开发软件采购	针对客户要求的部分成品系统或软件中非公司核心技术的部分，进行了外采，如信息植入、行为模型分析、大数据管理查询等，以完成客户合同中要求的全套软件交付使用。
4	外包	主要为网络安全科技馆一体化项目中的部分展项外包	网络安全科技馆项目工程量大、交付时间紧张，为缓解公司交付压力，对部分不涉及到公司核心技术的展示互动类展项直接进行了外采。
5	培训、运维服务等其他采购	主要指课程培训、运维等支撑服务	在公司线上线下课程、运维项目中，通过外聘讲师及相关人员等形式，缓解公司项目人手不足的压力。

二、主要供应商情况

上述五种采购所对应的主要供应商及发生的具体采购内容如下表所示：

采购类型	序号	供应商	主要采购内容
基础设施、网络环境等业务必须的支持性采购	1	上海术推科技服务事务所	VPS
	2	北京鹏途腾飞科技有限公司	动画视频制作及剪辑
	3	北京中顺诚科技有限公司	动画影片制作
	4	北京想联嘉业科技有限公司	VPS

持性采购	5	北京恒辉国信科技有限公司	视频录制制作
安全服务类采购	1	北京明略软件系统有限公司	搭建相应的环境对漏洞进行测试,并出具众测运营服务报告及漏洞报告
	2	随锐科技集团股份有限公司	设备漏洞挖掘和应用节点扫描探测
	3	安徽云探索网络科技有限公司	网络流量展示系统测试及开发服务
	4	深圳零天科技有限公司	技术服务
	5	奇安信科技集团股份有限公司	安全检测与测试服务
成品系统及系统开发采购	1	安徽云探索网络科技有限公司	指挥管控系统、移动通讯工具系统等
	2	北京坤元和讯技术有限公司	用户管理、用户交互、用户日志、宏观态势展示、安全数据抽取等系统版块
	3	厦门安胜网络科技有限公司	终端安全检测、远控系统
	4	西安长峰机电研究所	大数据实时存储及计算机系统、大数据采集与共享系统
	5	北京金晴云华科技有限公司	金晴云华高级威胁检测系统、服务器/高级威胁检测系统
外包	1	随锐科技集团股份有限公司	科技馆意识闯关、安全射击等趣味游戏模块开发
	2	观脉科技(北京)有限公司	网安科技馆 APT 攻击态势展示-威胁情报网关系统开发
	3	阿里云计算有限公司	魔镜、云安全风险、电商安全展项的软件开发
	4	北京百度网讯科技有限公司	科技馆 AI 手势识别、AI 图片识别等部分展项的制作
	5	上海且听网络技术服务中心	守护网站安全模块软件开发
培训、运维服务等其他采购	1	深圳奥联信息安全技术有限公司	网络安全视频课程、驻场服务等
	2	北京神州泰岳软件股份有限公司	专项技术培训、活动人员驻场服务等
	3	福建东诺科技有限公司	网络支撑与应急响应服务
	4	北京神州普天科技发展有限公司	安全培训服务
	5	山西观星科技有限公司	师资委派、赛题定制等

(3) 靶场实验室平台建设需采购装修工程的原因及采购金额,服务的提供方。

报告期间,公司其他类采购金额分别为 323.17 万元、525.17 万元、715.84 万元和 712.68 万元,其中因网络靶场系列产品业务发生的装修工程采购分别为 212.67 万元、29.07 万元、446.25 万元和 419.83 万元。公司所指发生装修工程采购的靶场实验室平台建设项目为有实体的靶场实验室一体化项目,包括无实体的网络靶场与有实体的实验室场地,因此需要对实验室环境进行装修。

报告期内发生装修工程采购的网络靶场系列产品业务及供应商与采购金额

如下：

单位：万元

序号	客户名称	2021年 1-6月	2020年	2019年	2018年	采购供应商
1	中国科学院信息工程研究所	388.29	-	-	-	北京银达兴业建筑工程公司
2	郑州高新产业投资集团有限公司	-	335.38	-	-	河南辰泰电子科技有限公司 河南省岁龙装饰有限公司 深圳市翌境科技有限公司 武汉红顶旭环境工程有限公司
3	南京市公安局	-	-	6.73	82.52	南京伟桥科技有限公司
4	乌鲁木齐市公安局	-	-	-	118.89	新疆汇鑫嘉业建筑装饰工程有限责任公司
5	宁德市公安局	-	85.97	-	-	福州泓睿之家装饰工程有限公司 宁德市蓝橡树装饰工程有限公司
6	龙岩市公安局	-	18.81	-	-	士林建设实业有限公司
7	大田县公安局	13.11	2.58	-	-	福建长城电子技术工程有限公司 宁德市蓝橡树装饰工程有限公司
8	安康市公安局	14.85	-	-	-	安康市水云间装饰工程有限公司
9	成都安思科技有限公司	-	-	13.96	-	福州泓睿之家装饰工程有限公司
10	呼和浩特铁路公安局	-	-	-	11.26	内蒙古东奥装饰工程有限公司
11	武汉信息传播职业技术学院	-	-	8.37	-	武汉千纳达科技有限公司 武汉腾奥装饰有限公司
12	中国人民解放军	3.58	-	-	-	福州瑞祥友佳家具有限公司
13	北京航空航天大学	-	3.51	-	-	佛山市上下和地毯有限公司
	合计	419.83	446.25	29.07	212.67	-

【核查程序】

1、了解与采购相关的关键内部控制，评价相关控制的设计，确定其是否得到执行，并测试相关内部控制的运行有效性；

2、获取发行人采购明细表，核查各类别采购的金额及占比，了解采购模式、主要供应商的合作背景、采购内容以及供应商的变动情况；对剔除“网络安全科技馆”项目影响后的硬件设备、软件及技术服务的采购金额及变动原因进行分析；

3、获取发行人与主要供应商的合同等，了解向主要供应商的采购内容、采购金额及各期主要供应商变动原因；

4、访谈相关业务负责人，了解软件及技术服务的具体内容及对应在产品/服务中的应用情况；

5、获取靶场实验室的销售合同及对应装修工程的采购合同，确认发行人采购装修工程是否符合销售合同要求和实际业务背景。

【核查意见】

经核查，保荐机构及申报会计师认为：

1、剔除“网络安全科技馆”项目影响，硬件设备、软件及技术服务的采购金额相对稳定且变动合理；

2、发行人采购软件和技术服务主要系受公司自身的资源调配、人力资源紧张和非公司擅长领域的技术要求等因素影响所致；

3、公司作为靶场实验室一体化项目的服务提供商，按照合同的约定作为向客户提供靶场实验室平台的装修工程服务，由于不具有上述业务的专业能力，向第三方采购上述服务。

7、关于集成商

根据申报材料：报告期各期对集成商客户的销售金额分别为 3,407.57 万元、5,382.09 万元和 1,424.45 万元，在非终端客户销售的情形下，部分销售合同中约定终端客户的验收报告是收入确认的主要依据，报告期内未获取终端客户验收报告的销售金额约为 2,000 万元，以集成商出具验收报告时点确认收入。

请发行人说明：（1）与集成商合作的业务模式，对集成商客户收入变动的原因，集成商终端客户与发行人客户是否存在重叠；（2）集成商销售模式下采用不同收入确认依据的原因，是否与合同约定一致，报告期各期集成商的退、换货情况。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见。

【回复】

请发行人说明：

（1）与集成商合作的业务模式，对集成商客户收入变动的原因，集成商终端客户与发行人客户是否存在重叠；

一、与集成商合作的业务模式

公司的客户按照行业可分为政府直属企业客户、政府部门、军队、集成商、院校、其他客户等。集成商是指通过采购软件、软硬件一体化产品以及服务等，销售给其他客户。

公司配合集成商获取网络安全产品和服务的相关需求，参与到和终端客户方案对接、产品测试并制定价格的过程中。在获取终端客户初步意向需求后，针对具体的参数和技术要求，公司制定前期方案及初步报价，并形成技术方案书及成本报价单。

部分终端客户基于集约性、便捷性和地域性的考虑，会通过集成商来统一购买。发行人提供的技术方案书及报价单会作为集成商方案的组成部分，一并参与到终端客户的招投标等过程。集成商获取订单并签订合同后，再向公司采购合同中的部分内容。

此外，集成商也会直接向公司采购网络安全产品和服务用于自身使用，包括采购安全实验室靶场系统、采购安全工具类产品和竞赛培训等服务自用。

二、对集成商客户收入变动的原因

（一）集成商客户收入按产品分类

按照产品类别划分，公司报告期内集成商客户的收入和占比情况如下：

单位：万元

分类	2021 年 1-6 月		2020 年	
	收入	占比	收入	占比
网络安全产品	1,466.44	18.02%	932.22	3.20%
其中：网络靶场系列产品	1,010.26	12.42%	773.10	2.65%
安全管控与蜜罐产品	456.18	5.61%	98.76	0.34%
安全工具类产品	-	0.00%	60.35	0.21%
网络安全服务	540.93	6.65%	492.23	1.69%
其中：安全防护系列服务	376.30	4.63%	252.78	0.87%
网络安全竞赛服务	-	0.00%	90.42	0.31%
其他服务	164.64	2.02%	149.03	0.51%
合计	2,007.37	24.67%	1,424.45	4.88%

（续上表）

分类	2019 年	2018 年
----	--------	--------

	收入	占比	收入	占比
网络安全产品	4,443.23	27.24%	2,802.55	15.53%
其中：网络靶场系列产品	2,263.71	13.88%	2,284.31	12.65%
安全管控与蜜罐产品	982.06	6.02%	36.83	0.20%
安全工具类产品	1,197.46	7.34%	481.41	2.67%
网络安全服务	938.86	5.76%	605.02	3.35%
其中：安全防护系列服务	503.87	3.09%	299.60	1.66%
网络安全竞赛服务	49.37	0.30%	81.89	0.45%
其他服务	385.61	2.36%	223.54	1.24%
合计	5,382.09	33.00%	3,407.57	18.88%

报告期内，公司集成商带来的销售收入分别为 3,407.57 万元、5,382.09 万元、1,424.45 万元和 2,007.37 万元，在收入总额中的占比分别为 18.88%、33.00%、4.88%和 24.67%。

2019 年集成商收入比 2018 年增加 1,974.52 万元，同比增长 57.94%，主要原因是 2019 年公司向厦门安胜网络科技有限公司销售安全管控与蜜罐产品 533.42 万元，向启明星辰安全销售安全工具类产品 639.70 万元，导致 2019 年当期的安全管控与蜜罐产品和安全工具类产品的收入较 2018 年度大幅增长。

2020 年集成商收入比 2019 年减少 3,957.64 万元，同比降低 73.53%，主要原因系同一政府机构的不同部门、不同项目往往面临着不同的项目需求，终端客户会结合项目的体量大小、复杂程度、可利用的资源、本地化服务需求等因素，选择集成商或由公司直接提供服务。例如，2019 年公司向北京华威益腾通讯技术有限公司销售网络靶场系列产品 838.00 万元，其终端客户为北京一三一八单位。2020 年公司根据北京一三一八单位的要求，直接向其销售网络靶场系列产品，实现网络靶场系列产品收入 693.04 万元。

2021 年 1-6 月集成商收入上涨，主要原因是 2021 年公司向网神信息销售网络靶场系列产品 443.65 万元以及安全管控与蜜罐产品 354.41 万元，向厦门安胜网络科技有限公司销售网络靶场系列产品 383.45 万元以及安全管控与蜜罐产品 66.37 万元，向成都天用唯勤科技股份有限公司提供安全防护系列服务 301.89 万元。因此，公司 2021 年通过集成商向重叠的终端客户销售的收入额增长。

报告期内，终端客户对网络安全产品和服务的需求存在短期波动。另外，终

端客户会自主选择直接向公司采购，或是选择集成商采购。因此报告期内公司集成商业务的收入存在波动。

（二）报告期向前五大集成商客户销售情况

2021 年 1-6 月前五大集成商客户收入明细如下：

单位：万元

序号	集成商名称	主要终端客户名称	业务类型	收入
1	网神信息技术（北京）股份有限公司	奇安信科技集团股份有限公司	网络靶场系列产品、安全管控与蜜罐	771.69
		公安单位	网络靶场系列产品	26.37
2	厦门安胜网络科技有限公司	福建省公安厅	网络靶场系列产品、安全管控与蜜罐	402.65
		厦门市公安局	网络靶场系列产品	47.17
		漳州市公安局	其他服务	19.45
3	成都天用唯勤科技股份有限公司	多家终端客户	安全防护系列服务	301.89
4	北京信安华宁信息技术有限公司	个人学员	其他服务	96.31
5	北京锐安科技有限公司	梧州市公安局	网络靶场系列产品	77.88
	合计			1,743.41

2020 年前五大集成商客户收入明细如下：

单位：万元

序号	集成商名称	主要终端客户名称	业务类型	收入
1	深圳万佳怡科技有限公司	润联软件系统（深圳）有限公司	网络靶场系列产品	123.89
2	浙江同力信息科技有限公司	杭州电子科技大学	网络靶场系列产品	115.04
3	方圆化集团有限公司	中国人民武装警察部队特种警察学院	网络靶场系列产品	79.65
4	上海安洵信息技术有限公司	广东省公安厅	安全工具类产品	59.96
		阜阳市公安局	安全管控与蜜罐产品	17.26
5	北京知道创宇信息技术股份有限公司	北京市对外服务办公室	安全防护系列服务	61.09
	合计			456.89

2019 年前五大集成商客户收入明细如下：

单位：万元

序号	集成商名称	主要终端客户名称	业务类型	收入
1	北京华威益腾通讯技术有限公司	北京一三一八单位	网络靶场系列产品	838.00

2	启明星辰安全	政企类用户	安全工具类产品、网络靶场系列产品、其他服务	659.51
3	厦门安胜网络科技有限公司	福建省公安厅	安全管控与蜜罐产品、网络靶场系列产品	577.66
		厦门市公安局	安全防护系列服务	61.58
		赣州市公安局	网络靶场系列产品	4.31
4	北京知道创宇信息技术股份有限公司	军队	网络靶场系列产品	262.35
5	河南信大网御科技有限公司	网络通信与安全紫金山实验室	网络靶场系列产品	251.18
	合计			2,654.59

2018 年前五大集成商客户收入明细如下：

单位：万元

序号	集成商名称	主要终端客户名称	业务类型	收入
1	金鹏电子信息机器有限公司	广州市公安局	网络靶场系列产品	697.01
2	启明星辰安全	政企类用户	安全工具类产品、安全防护系列服务、网络靶场系列产品、其他服务	503.66
3	南京烽火星空通信发展有限公司	吉林省公安厅	安全工具类产品	164.96
		汕头市公安局	网络靶场系列产品	126.69
		重庆市公安局	其他服务	4.72
4	湖南雨人网络安全技术股份有限公司	湖南省公安厅	网络靶场系列产品	258.62
5	北京信安华宁信息技术有限公司	信息产业信息安全测评中心	其他服务、网络靶场系列产品等	235.78
	合计			1,991.45

报告期内，公司以直销为主，集成商客户带来的销售收入分别为 3,407.57 万元、5,382.09 万元、1,424.45 万元和 2,007.37 万元，在收入总额中的占比分别为 18.88%、33.00%、4.88%和 24.67%。报告期的前五大集成商中，发行人共和 17 个集成商合作 49 个项目，各期和单一集成商合作的项目数量少，前五大集成商的波动受单一项目影响较大。

三、集成商终端客户与发行人客户的重叠情况

发行人报告期各期集成商的终端客户与发行人客户存在重叠，具体的情形如下：

单位：万元

	2021年1-6月	2020年	2019年	2018年
通过集成商向重叠的终端客户销售的收入额	1,410.41	315.67	2,261.06	1,878.41
当期收入总额	8,136.08	29,164.20	16,308.54	18,051.03
占比	17.34%	1.08%	13.86%	10.41%

报告期内，公司通过集成商向重叠的终端客户销售的收入额分别为 1,878.41 万元、2,261.06 万元、315.67 万元和 1,410.41 万元，在收入总额中的占比分别为 10.41%、13.86%和 1.08%和 17.34%。2019 年占比较高的主要原因是 2019 年公司通过厦门安胜网络科技有限公司向福建省公安厅销售安全管控与蜜罐产品 533.42 万元，同时公司直接向福建省公安厅销售网络靶场系列产品 130.53 万元。2019 年公司通过河南信大网御科技有限公司向网络通信与安全紫金山实验室销售网络靶场系列产品 251.18 万元，同时公司直接向网络通信与安全紫金山实验室提供安全防护系列服务 186.32 万元。因此，公司 2019 年通过集成商向重叠的终端客户销售的收入额增长。

2021 年 1-6 月占比较高的主要原因是 2021 年公司通过厦门安胜网络科技有限公司向福建省公安厅销售网络靶场系列产品 336.28 万元以及安全管控与蜜罐产品 66.37 万元，同时公司也直接向福建省公安厅销售网络靶场系列产品 130.53 万元。公司通过珠海慧港信息技术有限公司向广东省公安厅销售安全管控与蜜罐产品 67.45 万元，同时公司报告期内直接向广东省公安厅提供安全防护系列服务 668.30 万元、网络靶场系列产品 350.17 万元和安全管控与蜜罐 861.34 万元。因此，公司 2021 年通过集成商向重叠的终端客户销售的收入额增长。

发行人报告期集成商的终端客户中，重叠部分主要是公安等政府部门，终端客户部分项目由发行人直接承接，部分项目由集成商承接后转向发行人采购，集成商终端客户与发行人客户存在重叠。具体而言，重叠的主要原因如下：

1、项目内容

主要原因系同一政府机构的不同部门、不同项目往往面临着不同的项目需求，终端客户会结合项目的体量大小、复杂程度、可利用的资源、本地化服务需求等因素，选择集成商或由发行人直接提供服务。如果项目内容大部分是发行人主营业务范围中的网络安全产品和服务，一般直接向发行人采购。如果整体项目是包

含装修建设、施工、网络安全产品等内容的总包合同，一般由集成商总体负责，仅向发行人采购其中的网络安全产品和服务。

2、项目的延续性

一般而言，实验室集成建设类项目，由本地集成商总体负责，包含实验室装修、平台项目等内容，其中的靶场平台从发行人处采购。后续模块升级、更新维护等内容一般直接向发行人采购。

(2) 集成商销售模式下采用不同收入确认依据的原因，是否与合同约定一致，报告期各期集成商的退、换货情况。

一、公司集成商销售模式收入确认方法和依据

公司集成商销售模式的收入确认方法和依据如下：

主营业务分类	收入确认方法	收入确认依据
网络靶场系列产品	软件产品的控制权已经转移，软件安装调试完成，取得客户出具的终验报告时确认收入	客户出具终验报告时确认收入
安全管控与蜜罐产品	软件产品的控制权已经转移，软件安装调试完成，取得客户出具的终验报告时确认收入	客户出具终验报告时确认收入
安全工具类产品	软件产品的控制权已经转移，软件安装调试完成，取得客户出具的终验报告时确认收入	客户出具终验报告时确认收入
网络安全竞赛	赛事举办结束后取得委托方出具的终验报告时确认收入	客户出具终验报告时确认收入
安全防护系列服务	按照服务期间平均确认收入	服务期内每月确认收入

公司集成商销售模式采用的收入确认方法及依据如上表所示，且均与直接销售的相关原则和收入确认依据一致。

二、公司集成商销售模式采用的收入确认证据与相关合同约定的匹配性

(一) 合同约定的验收条款及需最终用户参与的情况

根据公司与集成商签署的销售合同约定，验收方式通常有两种，一是由集成商客户进行项目的验收工作，二是由终端客户参与项目的验收工作。

1、由集成商验收的销售合同一般对验收条款的约定如下：乙方（公司）交货至甲方（集成商）指定地点，安装调试成功正常运行并交付使用后，乙方提出验收申请，验收合格的，甲、乙双方代表签署验收报告。

2、报告期内，公司集成商销售模式下，存在部分销售合同中约定，项目的最终验收需要由终端客户参与和确认，具体情况如下：

单位：万元

项目	2021 年 1-6 月	2020 年	2019 年	2018 年
主营业务收入	8,136.08	29,164.20	16,308.54	18,051.03
集成商收入	2,007.37	1,424.45	5,382.09	3,407.57
集成商业收入的占比	24.67%	4.88%	33.00%	18.88%
集成商销售模式下，需要终端客户验收的项目收入	589.63	244.15	1,356.10	721.72
集成商销售模式下，需要终端客户验收的项目数量	7	8	17	11
集成商销售模式下，需要终端客户验收的项目收入在主营业务收入中的比例	7.25%	0.84%	8.32%	4.00%
集成商销售模式下，明确要求终端客户出具验收报告的项目数量	-	-	-	-

报告期内，公司集成商收入分别为 3,407.57 万元、5,382.09 万元、1,424.45 万元和 2,007.37 万元，在主营业务收入中的占比分别为 18.88%、33.00%、4.88% 和 24.67%。在集成商业模式下，部分集成商的销售合同中约定“本项目最终通过客户验收方视为本合同服务内容验收合格”、“最终用户针对该项目最终验收合格后，才视为乙方的服务完成”、“采购的产品是提供给最终客户使用的，验收以最终客户的要求为准”、“产品的验收标准：以最终用户方确认为合格为验收标准”等条款，均未明确要求需要终端客户出具验收报告。集成商销售模式下，需要终端客户验收的项目产生的收入额分别为 721.72 万元、1,356.10 万元、244.15 万元和 589.63 万元，在主营业务收入中的占比分别为 4.00%、8.32%、0.84% 和 7.25%。公司需要终端客户参与项目验收的项目较少，占比较低。

（二）公司收入确认采用集成商出具的终验报告

公司集成商模式下，存在部分合同需要终端客户验收，但均未明确要求需要终端客户出具验收报告。虽然终端用户未对公司出具验收报告，但集成商对公司项目进行验收前，已经过终端客户的验收，符合行业惯例。针对需要终端客户验收的项目，公司确认收入以集成商出具的终验报告为准，主要原因如下：

1、行业惯例一般为最终客户给集成商客户验收后，集成商客户才给公司进行验收。公司历史上未曾出现通过集成商的最终验收后，未通过最终客户验收的情况。报告期内已获取集成商说明函的项目收入在需要终端客户验收的项目收入中的占比为 79.36%。公司与集成商签署的合同中明确约定终端客户需要验收项

目的，由于公司不属于最终客户的合同约定供应商，最终用户无单独向公司出具验收报告的义务。集成商在通过终端客户的验收后，向公司出具验收报告。

2、公司拿到集成商客户的终验报告时，公司已将所有外购的硬件服务器装载上自主开发的软件移交给客户，并完成安装调试工作，公司负责的独立系统已经按照合同的约定完成了试运行工作，公司已完成了合同中约定的履约义务。同时，项目完成终验时，已完成合同中约定的全部履约义务，最终客户已经取得相关软件的控制权，即公司已经将系统交付给最终客户，最终客户已经接受并完全控制该软件产品，最终客户能够从中获得几乎全部经济利益，公司享有现时收款权利，满足收入确认的要求。

（三）同行业公司确认收入情况

根据同行业公司公开信息，安恒信息、奇安信均采用了直销与渠道代理销售相结合的销售模式，收入确认依据为收到验收报告。

安恒信息收入确认依据如下：

业务类别	销售模式	收入确认原则
网络信息安全产品	直销	(1) 若合同未约定由安恒信息负责安装实施，获得到货签收单后一次性确认收入； (2) 若合同约定由安恒信息负责安装实施，收到验收报告后一次性确认收入。
	渠道销售	(1) 若合同未约定由安恒信息负责安装实施，获得到货签收单后一次性确认收入； (2) 若合同约定由安恒信息负责安装实施，收到验收报告后一次性确认收入。
网络信息安全服务	直销	(1) 按次提供服务的：收到验收报告或服务确认单一次性确认收入； (2) 有服务期限的：按约定的服务期限摊销。
	渠道销售	(1) 按次提供服务的：收到验收报告或服务确认单一次性确认收入； (2) 有服务期限的：按约定的服务期限摊销。

注：根据安恒信息招股说明书的披露，安恒信息根据不同客户的规模、需求特性，选择与不同特点的系统集成商进行渠道业务合作。

根据奇安信招股说明书的披露，奇安信收入分为直销收入和渠道（集成商）收入，奇安信收入确认依据如下：

业务类别	情形	收入确认原则
安全产品收入	不需安装调试	按合同约定将安全产品转移给对方后确认收入。
	需安装调试	按合同约定在项目实施完成后并经客户验收合格后确认

		收入。
安全服务收入 硬件及其他收入 使用费收入	合同已约定验收条款	在服务已经提供，并经客户验收后确认收入。
	未约定验收条款	在合同约定的服务期限内平均确认收入。 按照安全产品收入的确认原则确认收入。 根据有关合同或协议，按权责发生制确认收入。

由上表可知，安恒信息、奇安信等上市公司在直销模式与渠道销售模式下的收入确认原则均无区别。

综上，公司集成商模式下，存在部分合同需要终端客户验收，但均未明确要求需要终端客户出具验收报告。虽然终端用户未对公司出具验收报告，但考虑到行业惯例一般为最终客户给集成商验收后，集成商才给公司进行验收。公司拿到集成商的终验报告时，已满足确认收入的要求。因此针对需要终端客户验收的项目，公司确认收入以集成商出具的终验报告为准，符合行业惯例，符合会计准则的要求。

三、报告期各期集成商的退、换货情况

报告期内，公司承做的集成商项目未发生因未通过最终用户验收而退、换货的情形。

【核查程序】

- 1、访谈公司的主要集成商，了解集成商在交易中承担的主要职能；
- 2、访谈发行人总经理、销售负责人及相关业务人员，了解报告期内公司集成商合作的商业模式、集成商销售收入变化的情况及原因；
- 3、获取发行人收入明细表，了解行业收入分布情况，以及直接客户和集成商的收入情况；了解公司直接客户和集成商的收入重叠的情况，分析重叠原因的合理性；分析公司的直接客户与通过集成商销售的最终客户的结构差异情况；
- 4、取得并检查集成商销售合同、签收单、验收单等资料，核查公司集成商收入确认政策是否与合同约定一致；检查期后项目情况，是否存在集成商退换货的情形；
- 5、查阅同行业上市公司收入确认原则及确认依据，结合公司自身业务实际情况，分析公司收入确认方法的合理性。
- 6、获取集成商出具的验收情况说明函，确认项目是否完成，并确认终端客户的验收情况及验收时间，进而核查收入是否符合收入确认条件、是否确认至正

确的期间。报告期内已获取集成商说明函的项目收入在需要终端客户验收的项目收入中的占比为 79.36%。

【核查意见】

经核查，保荐机构和申报会计师认为：

1、公司集成商的合作模式一般是通过参与终端客户的招投标等过程来获取业务；报告期内集成商收入变动的原因具有合理性；由于终端客户不同项目的需求存在差异，公司集成商终端客户与公司的直接客户存在重叠的情况；

2、公司集成商销售业务的收入确认原则及取得的收入确认证据与合同条款相匹配，与直接销售模式的相关原则和依据一致，且与同行业公司收入确认原则一致。报告期内，公司承做的集成商项目未发生因未通过最终用户验收而退、换货的情形。

8、关于收入

8.1、收入确认政策

根据申报材料：（1）网络靶场产品、安全管控与蜜罐产品和安全工具类产品、科技体验教育平台、网络安全竞赛服务在取得终验报告时确认收入；（2）报告期各期软件收入金额分别为 7,515.23 万元、6,613.62 万元和 14,759.48 万元；服务收入金额分别为 5,450.01 万元、8,319.99 万元和 10,818.34 万元；硬件收入金额分别为 5,085.79 万元、1,374.92 万元和 3,586.38 万元；（3）报告期内公司指定采购软件及技术服务的比例分别约为 35%、20%和 20%；部分客户明确指出所需产品的技术指标和版本；部分合同约定了采购内容包括“外星人便携式计算机、苹果便携式计算机、办公桌、文件保密柜…”等，且单独约定价格；（4）部分合同约定“硬件设备 3 年免费维护、更换配件服务，系统软件 3 年免费维护和升级”、“3 年内提供成本价升级服务”、“项目开始至验收后 1 年内，提供 3 人的技术驻点服务”；（5）部分技术开发委托合同中约定“利用研究开发经费购置的设备、器材、资料的使用权属于发行人”、“达到技术指标和参数并交付给客户，交付成果为光盘形式”；（6）对于部分成熟产品，公司采用试用推广模式，先将成熟产品提供给最终客户试用。

请发行人说明：（1）软件、服务、硬件收入的具体划分标准及对应的成本、毛利率情况；软件收入金额与增值税税收优惠金额的匹配性；（2）指定采购的

情况下采用总额法确认收入是否符合企业会计准则的规定；（3）技术开发委托合同中研究开发经费的资金来源，购置的设备、器材、资料和所有权归属及会计核算情况；（4）验收后 1 年的技术驻点服务、成本价升级服务相关的会计核算情况，试用商品的会计核算、收回后的处理机制及财务影响。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见。

【回复】

请发行人说明：

（1）软件、服务、硬件收入的具体划分标准及对应的成本、毛利率情况；软件收入金额与增值税税收优惠金额的匹配性；

一、软件、服务、硬件收入的具体划分标准及对应的成本、毛利率情况

单位：万元

分类	2021 年 1-6 月			2020 年		
	收入	成本	毛利率	收入	成本	毛利率
软件	4,203.39	1,142.76	72.81%	16,061.85	3,085.50	80.79%
服务	3,238.56	1,742.03	46.21%	10,568.66	7,563.04	28.44%
硬件	694.13	632.25	8.91%	2,533.69	2,067.32	18.41%
合计	8,136.08	3,517.04	56.77%	29,164.20	12,715.86	56.40%

（续上表）

分类	2019 年			2018 年		
	收入	成本	毛利率	收入	成本	毛利率
软件	7,402.62	1,811.55	75.53%	8,249.11	1,242.50	84.94%
服务	7,482.48	2,602.45	65.22%	5,022.01	1,549.42	69.15%
硬件	1,423.44	1,017.84	28.49%	4,779.91	3,066.72	35.84%
合计	16,308.54	5,431.84	66.69%	18,051.03	5,858.64	67.54%

软件、服务、硬件收入的具体情况如下：

1、软件收入

公司软件收入是指以公司自行开发的软件著作权对应的软件产品进行销售，和根据客户需求，在公司自有标准化产品的基础上进行定制化开发的软件产品销售形成的收入。

公司软件收入报告期内分别为 8,249.11 万元、7,402.62 万元、16,061.85 万元和 4,203.39 万元，2019 年软件收入和 2018 年相比下降 10.26%，主要原因系昆山九华电子设备厂的基于网络数据处理技术-原型开发项目收入金额为 2,100 万元，由于项目调试运行未在 2019 年完成，项目于 2020 年最终验收，未在 2019 年确认收入；2020 年软件收入较高，主要系公司承接了网络安全科技馆项目，该项目软件收入占比较高。受业务季节性影响，2021 年 1-6 月软件收入较其他年度全年减少明显。

公司软件收入毛利率分别 84.94%、75.53%、80.79%和 72.81%，毛利率较高系公司销售自有软件产品和定制化软件时，主要的成本构成为人工及对应装载的硬件服务器，其他成本较少导致了综合毛利率偏高，2019 年和 2021 年 1-6 月软件收入毛利率较其他年度下降，主要原因系高度定制化的项目拉低了综合毛利率。

2、服务收入

公司服务收入是指公司在客户的委托下执行安全防护系列、线上线下网络安全培训、赛事运营等服务形成的收入。

公司服务收入报告期内分别为 5,022.01 万元、7,482.48 万元、10,568.66 万元和 3,238.56 万元，服务收入逐年提高，主要原因系公司在网络培训领域、网络安全赛事领域口碑逐年增加，承接服务业务逐年提高导致服务收入逐年增加。受业务季节性影响，2021 年 1-6 月服务收入较其他年度全年减少明显。

公司 2020 年的服务收入较高，主要原因系网络安全科技馆项目确认了服务收入 3,673.10 万元。根据合同约定，公司需要根据甲方要求对工作内容，进行配套的管理和协调，并同时提供配合服务工作，主要包括：负责信息安全展示软硬件展品设计及研发、展品制作（含购置）、系统安装及调试、数字化解决方案、土建总包等工作的总体协调、及分包单位的协调，在施工现场对展品制作安装单位和其它专业分包商及有关施工单位进行总体管理、协调和服务，设计顾问咨询服务，对甲方相关人员的培训及技术指导，以及质保期内的维修保养等。

网络安全科技馆项目的服务收入主要系公司在网络安全科技馆项目中承担的展品服务、管理服务和设计服务，该部分确认收入金额为 2,215.46 万元。服务成果主要系展品的设计、项目现场的组织和管理等。此外，网络安全科技馆项目的服务收入还包括多媒体收入，主要系公司在网络安全科技馆项目中承担的多媒

体展品的制作，该部分确认收入金额为 1,457.64 万元，交付成果系多媒体产品的所有权。

服务毛利率报告期内分别为 69.15%、65.22%、28.44%和 46.21%，2018 年、2019 年公司服务毛利率较高，主要原因系服务收入对应的成本是人工薪酬，以及部分非公司领域的外包，服务业务的收入技术附加值较高，毛利率较高。

2020 年公司服务毛利率直线下降，主要原因网络安全科技馆项目，由于公司不具备影视制作能力及展品制作能力，故公司将该项目涉及的服务全部进行对外采购，涉及金额 3,673.20 万元，因项目周期较短，购置价格较高，毛利率较低，拉低了 2020 年整体服务收入的毛利率。

2021 年 1-6 月服务毛利率较 2020 年有所提高，但低于 2018 年和 2019 年的毛利率，主要原因受公司 2021 年承接的中海油信息科技有限公司的集团公司综合信息服务项目及“纵横比赛网络大赛”、“红明谷杯”网络赛事服务项目影响。中海油信息科技有限公司项目中，公司出于及时交付和战略客户项目建设效果的考虑进行了部分采购，且考虑到战略客户后续商机拓展定价较低，因此导致该项目服务收入毛利率仅为 10.06%；网络赛事服务项目中，公司提供赛事举办服务，同时达到宣传公司的目的，因此公司承担了该类项目的赛事奖金，拉低了 2021 年 1-6 月服务业务综合的毛利率。

公司网络安全竞赛服务主要系为客户提供网络安全赛事解决方案，通常包括赛事策划、赛制设计、平台开发、比赛培训、赛题制作、技术支持等服务，公司绝大多数网络安全竞赛服务均由主办方提供奖金，但有部分网络安全竞赛服务业务中公司会作为的网络安全竞赛总包方负责赛事整体的设计、组织与实施，其中 8 个项目也包含了赛事奖金支付，报告期内公司网络安全竞赛服务收入情况和需要承担赛事奖金的项目数量规模情况如下：

单位：万元

项目	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
网络安全竞赛服务相关收入	707.43	1,046.53	809.37	899.68
网络安全竞赛服务相关成本	362.45	398.35	273.48	307.80
毛利率	48.76%	61.94%	66.21%	65.79%
项目数量	2	1	3	2
涉及收入金额	371.05	33.68	94.25	169.80

相关奖金支出	51.00	4.96	9.12	28.03
--------	-------	------	------	-------

如上表所示，报告期内公司有 8 个网络安全竞赛服务项目为比赛选手提供奖金，奖金金额较小。比赛项目中，多数奖金由主办方支付，但也存在少部分奖金由公司支付，符合行业惯例。在销售合同中约定客户将赛事奖金作为合同的服务内容总包给公司，公司将赛事奖金费用作为对应的项目的营业成本进行核算。主要考虑因素如下：

A、公司承担赛事奖金的网络安全竞赛服务项目均在合同中明确了约定了公司需要承担需提供参赛选手奖金的责任和义务。

B、公司为赛事举办的总包方，如赛事评分及赛事奖金的支付出现问题，由公司承担责任；

C、公司承担赛事奖金的网络安全竞赛服务项目中，除武汉市 2018 年黄鹤杯网络安全大赛活动服务合同外，其他项目合同未明确约定奖金金额，公司对赛事的评分及具体奖金金额具有自主决定权。

在对 2020 年网络安全科技馆项目、2021 年中海油信息科技有限公司集团公司综合信息服务项目及“纵横杯网络安全竞赛”、“红明谷杯”网络赛事服务项目所确认的服务收入进行剔除后，报告期内公司服务收入毛利率基本保持稳定，如下表所示：

单位：万元

项目	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
剔除前				
服务收入	3,238.56	10,568.66	7,482.48	5,022.01
服务毛利率	46.21%	28.44%	65.22%	69.15%
剔除后				
服务收入	2,281.85	6,895.46	7,482.48	5,022.01
服务毛利率	59.59%	62.26%	65.22%	69.15%

3、硬件收入

公司硬件收入是指公司在签订软件开发合同后，配套采购的服务器、电脑等硬件设备，以及合同交付清单中约定加工和灌装后的硬件为主的产品形成的收入。

公司硬件收入报告期内分别为 4,779.91 万元、1,423.44 万元、2,533.69 万元和 694.13 万元，公司硬件收入增幅变动主要受各期承接项目的不同导致，2018

年硬件收入较高主要系公司承接了南京市公安局、广东省公安厅等公安系统客户的网络安全实验室或靶场建设等一体化建设项目，此类项目中包含实验室及靶场环境建设、硬件设施等需求，因此实验室环境及基础设施建设发生硬件设备收入 2,865.36 万元。2020 年硬件收入较 2019 年有所提高，主要因承接各地公安系统实验室及网络安全平台建设项目发生硬件设备收入 974.70 万元、网络安全科技馆项目发生硬件设备收入 571.79 万元所致。2021 年 1-6 月公司硬件产品毛利率持续下降，原因是针对参数要求较高的部分硬件产品，公司为了保证与客户良好的合作关系将硬件产品进行了进一步升级，导致硬件成本较高，拉低了硬件产品的综合毛利率。

公司硬件毛利率报告期内分别为 35.84%、28.49%、18.41%和 8.91%。公司硬件毛利率较高的主要原因在于公司不是简单的硬件购销业务，在外购硬件的基础上进一步加工和灌装，最终该部分体现为以硬件为主的软硬件一体化产品。硬件毛利率较高主要项目的具体情况如下：

单位：万元

序号	会计期间	客户名称	项目名称	硬件收入	硬件毛利率	硬件毛利率较高的主要原因
1	2021 年 1-6 月	中国人民解放军 32057 部队	网络安全测试系统	26.55	45.28%	硬件部分主要是公司采集并分析数据后，加工灌装后的硬件设备，因此硬件毛利率较高。
2	2021 年 1-6 月	中国人民解放军 32057 部队	网络安全测试系统	7.08	45.28%	硬件部分主要是公司采集并分析数据后，加工灌装后的硬件设备，因此硬件毛利率较高。
3	2020 年	杭州市公安局	杭州市公安局网络靶场项目	230.97	61.70%	硬件收入主要是加工和灌装公司基础设施资源管理子系统、综合配置管理维护子系统、任务综合统筹子系统、环境仿真应用子系统后的专用管理硬件设备，因此硬件毛利率较高。
4	2020 年	山西省公安厅	网络平台一期项目	149.56	32.22%	硬件收入主要是以硬件为开发载体的软硬件支撑平台，包括指挥调度、演练和展示等功能模块，不是简单的通用硬件购销业务。
5	2020 年	淮安市公安局	网络安全设备采购项目	127.43	26.23%	硬件收入主要是含有公司自有软件部分的软硬

						件一体化产品包括网络工具箱系统 V2.0、互联网空间探测系统 V3.0 等自有软件，因此硬件毛利率较高。
6	2020 年	贵州省公安厅	网络靶场项目	84.48	49.36%	硬件部分主要是包含靶场指挥调度系统、测试平台等软硬件一体化设备，因此毛利率较高。
7	2020 年	中国银联股份有限公司	2019 年安全攻防竞赛及实训平台建设 IT 软硬件采购合同	66.37	41.28%	硬件收入主要是灌装公司 e 春秋软件平台后的软硬件一体化产品，因此硬件毛利率较高。
8	2020 年	广发银行股份有限公司	广发银行网络安全分罩设备购销合同	63.72	64.41%	硬件收入主要是安全罩分罩设备，包括针对用户需求定制开发的与安全罩总控对接的专门软件系统及适配处理能力的硬件，软硬一体交付。
9	2020 年	宁波市公安局	数据采集与系统项目	61.68	58.56%	硬件部分主要是公司采集并分析数据后，加工灌装后的硬件设备，因此硬件毛利率较高。
10	2019 年	厦门安胜网络科技有限公司	设备采购项目	272.55	58.17%	硬件收入主要是网络数据系统，系定制开发的软硬件一体设备，因此硬件毛利率比较高。
11	2019 年	中国人民解放军	智能项目组网	69.99	25.23%	硬件收入主要是以硬件为开发载体的软硬件支撑平台，不是简单的通用硬件购销业务。
12	2019 年	武汉大学	网络攻防靶场平台	51.86	21.89%	硬件收入主要是以硬件为开发载体的软硬件支撑平台，不是简单的通用硬件购销业务。
13	2019 年	公安部十一局	内网漏洞检测工具	47.22	84.83%	硬件收入主要是公司定制开发的内网漏洞检测工具，因此硬件毛利率较高。
14	2019 年	哈尔滨工业大学（深圳）	哈尔滨工业大学（深圳）安全实验室项目	44.78	24.72%	硬件收入主要是以硬件为开发载体的软硬件支撑平台，不是简单的通用硬件购销业务。
15	2019 年	北京兆维电子（集团）有限责任公司	网络攻防试验平台（e 春秋网络安全实验室培训平台 V3.0）	15.04	97.83%	硬件收入主要是灌装公司 e 春秋软件平台后的软硬件一体化产品，因此硬件毛利率较高。
16	2019 年	华中科技大学	攻防竞赛服务器	13.79	65.91%	硬件收入主要是灌装公司 e 春秋软件平台后的

						软硬件一体化产品，因此硬件毛利率较高。
17	2018年	南京市公安局	网络安全实验室建设项目	895.47	22.64%	硬件收入主要是实验室建设项目的专用服务器、终端设备和定制化装修等，因此硬件毛利率较高。
18	2018年	北京启明星辰信息安全技术有限公司	专用装备项目	252.60	45.72%	硬件收入主要是含有公司自有数据资源库专业存储设备、数据资源库专用分析设备和数据资源数据推理及可视化装备，因此硬件毛利率较高。
19	2018年	广东省公安厅	网络安全态势感知系统	236.15	52.41%	硬件收入主要是以硬件为开发载体的软硬件融合设备，包括整个系统平台内的专用设备、负载均衡、防火墙等，不是简单的通用硬件购销业务，因此硬件毛利率较高。
20	2018年	广东省公安厅	广东实验室二期	203.19	33.73%	硬件收入主要是含有业务系统、指挥管理系统的软件一体化设备，因此硬件毛利率较高。
21	2018年	安溪县公安局	网络安全实验室专用设备	190.30	27.61%	硬件收入主要是以硬件为主的软硬件支撑平台，包括灌装软件后的防火墙、光闸，并且对安全软件调试和联调，因此硬件毛利率较高。
22	2018年	广东广安信息发展公司广州分公司	运维安全保障区/综合网络技术应用系统/业务指挥管控系统/业务可视化综合展示系统	187.44	77.61%	硬件部分主要含有综合网络技术运维系统、资源调度子系统、网络运维资源软件、业务指挥管理系统、业务可视化综合展示系统的专用管理硬件设备，因此硬件毛利率较高。
23	2018年	江西省公安厅	江西省公安厅网安总队实验室专用设备	178.12	79.79%	硬件收入主要是以硬件为开发载体的软硬件支撑平台，包括网络管理系统、安全审计系统等，因此硬件毛利率较高。
24	2018年	北京市公安局	专项采购项目	145.52	61.45%	硬件收入主要是终端远程控制工具及流量管理工具和流量生成套件，

						其中公司根据客户实际业务需求定制研发部分功能，因此硬件毛利率比较高。
25	2018年	丽水市公安局	网络流量分析系统丽水市公安局项目	114.06	93.71%	硬件收入主要是软硬一体设备，根据客户的业务需求及实际使用要求针对软硬件进行定制开发。
26	2018年	公安部十一局	网络远程运维管理工具和网络远程监控工具	100.34	83.38%	硬件收入主要是网络远程运维管理工具和网络远程监控工具系统，因此硬件毛利率较高。
27	2018年	淮安市公安局	实验室建设项目	85.34	29.13%	硬件收入主要是平台服务器，WIFI 设备、调取系统和取证系统，因此硬件毛利率较高。
28	2018年	四川省畅达运输有限责任公司	网络敏感数据侦控系统 V1.8	80.12	81.86%	硬件收入主要是软硬一体设备，根据客户的业务需求及实际使用要求针对软硬件进行定制开发。
29	2018年	南京东大智能化系统有限公司	东南大学实验室项目	72.41	59.76%	硬件部分主要是灌装公司 e 春秋软件平台的软硬件一体化设备，因此毛利率较高。
30	2018年	北京神州泰岳教育科技有限公司	网络安全人才培养项目	63.70	53.46%	硬件部分主要是灌装公司 e 春秋软件平台的软硬件一体化设备，因此毛利率较高。
31	2018年	南京科讯次元科技有限公司	网络靶场平台采购项目	34.36	70.48%	硬件部分主要是灌装公司 e 春秋软件平台的软硬件一体化设备，因此毛利率较高。
32	2018年	广东电网有限责任公司信息中心	2018 年网络安全软硬件采购项目/APT 风险检测设备（慧眼高级威胁检测）	31.90	75.18%	硬件收入主要是包括慧眼 APT 高级威胁检测系统及相应配套处理能力的硬件设备，软硬一体交付。
33	2018年	北京南瑞怡和环保科技有限公司	Web 安全漏洞利用套件采购	30.17	84.46%	硬件部分主要是灌装公司 e 春秋软件平台的软硬件一体化设备，因此毛利率较高。
34	2018年	北京启明星辰信息安全技术有限公司	信息安全实验室建设项目	25.64	53.82%	硬件收入主要是以硬件为开发载体的软硬件支撑平台，不是简单的通用硬件购销业务。
35	2018年	北京诚智久安交通	e 春秋网络安全实验室攻防演	25.55	96.23%	硬件收入主要是以硬件为开发载体的软硬件支

		工程有限 公司	练平台 V2.0/智 能路侧单元/通 用交通信息采 集器			撑平台，不是简单的通 用硬件购销业务。
36	2018 年	北京市对 外服务办 公室	e 春秋网络安全 实验室培训平 台 V3.0/专用硬 件设备	21.55	47.14%	硬件收入主要是以硬件 为开发载体的软硬件支 撑平台，不是简单的通 用硬件购销业务。
	合计			4,307.03		

2020 年公司硬件毛利率下降的主要原因是网络安全科技馆项目，公司对外采购大量的硬件展品，该部分确认收入金额为 570.36 万元，因项目周期较短，购置价格较高，毛利率较低，拉低了 2020 年整体硬件收入的毛利率。

剔除掉以上列表项目后，报告期内公司硬件毛利率分别为 16.20%、15.76%、5.49%和 7.06%。公司硬件部分的收入、成本和毛利率具体如下：

单位：万元

分类	2021 年 1-6 月			2020 年		
	收入	成本	毛利率	收入	成本	毛利率
硬件	694.13	632.25	8.91%	2,533.69	2,067.32	18.41%
剔除毛利率偏高的项目	33.63	18.40	45.28%	784.22	413.83	47.23%
剔除后的硬件	660.50	613.85	7.06%	1,749.47	1,653.50	5.49%

(续上表)

分类	2019 年			2018 年		
	收入	成本	毛利率	收入	成本	毛利率
硬件	1,423.44	1,017.84	28.49%	4,779.91	3,066.72	35.84%
剔除毛利率偏高的项目	515.24	252.77	50.94%	2,973.94	1,553.31	47.77%
剔除后的硬件	908.20	765.07	15.76%	1,805.97	1,513.42	16.20%

二、软件收入金额与增值税税收优惠金额的匹配性；

(一) 公司报告期内的软件业务收入情况

公司报告期内的软件业务收入分类情况如下：

单位：万元

分类	2021 年 1-6 月	2020 年	2019 年	2018 年
享受即征即退的软件销售业务收入	3,065.05	4,840.29	4,210.48	5,937.22
其他软件销售业务	1,138.34	11,221.56	3,192.14	2,311.89

收入				
小计	4,203.39	16,061.85	7,402.62	8,249.11

公司报告期内的软件业务收入主要包括享受即征即退的软件销售业务收入和其他软件销售业务收入。享受即征即退的软件销售业务收入是指公司受托开发软件产品，可享受增值税即征即退的税收优惠。其他软件销售业务是指公司在自有软件产品和其他软件产品的基础上进行二次开发并形成独立产品对外销售，而非单纯地外采软件进行销售。

根据《财政部、国家税务总局关于软件产品增值税政策的通知》(财税〔2011〕100号)的相关规定，公司软件销售业务收入享受增值税即征即退的税收优惠。

(二) 公司软件收入金额与增值税税收优惠金额的匹配性

1、报告期内软件收入金额、增值税申报金额及税收优惠金额

报告期内软件收入金额、增值税申报金额及税收优惠金额情况如下：

单位：万元

项目	序号	2021年 1-6月	2020年	2019年	2018年	小计
账面软件销售收入	a	3,065.05	4,840.29	4,210.48	5,937.22	18,053.04
可申报即征即退的软件销售收入与实际申报即征即退的软件销售收入的时间性差异	b	-486.79	2,159.11	372.62	-2,052.01	-7.07
合并范围内抵消的可免税软件开发收入	c	-	165.83	28.79	147.93	342.55
当期申报即征即退的软件销售收入	d=a+b+c	2,578.26	7,165.23	4,611.89	4,033.14	18,388.52
当期申报即征即退的软件销售收入的销项税额[注]	e	335.17	901.4	597.17	653.14	2,486.88
当期申报即征即退的软件销售收入的进项税额	f	1.61	2.08	2.23	2.25	8.17
当期应收的退税款金额	g=(e-f) -d*3%	256.22	684.48	455.91	529.87	1,926.48
当期收到的以前年度的退税款金额	h	282.23	251.26	195.35	467.24	1,196.08
当期收到的应收的退税金额	i	210.92	402.25	204.65	334.52	1,152.34
当期应收暂未收到的退税款金额	j	45.14	282.23	251.26	195.35	773.98
计入当期其他收益的税收	k	493.14	653.51	400.00	801.76	2,348.41

项目	序号	2021 年 1-6 月	2020 年	2019 年	2018 年	小计
返还金额						
差异	$I = (h + i) - k$	-	-	-	-	-

注：公司销售自行开发生产的软件产品，按 13% 税率征收增值税（2018 年 5 月 1 日至 2019 年 3 月 31 日为 16%、2018 年 5 月 1 日前为 17%）

（1）报告期各期，可申报即征即退账面软件收入与当期申报即征退即软件收入之间的差异主要系公司收入确认时点与增值税纳税义务发生时点存在时间性差异所致。

（2）报告期各期期末存在应收未收的退税款，主要原因系主管税务局返还税款存在一定的时间间隔。公司已于 2021 年 8 月收到了税务部门返还的 2021 年 6 月末应收但暂未收取的即征即退款项 45.14 万元。报告期内，公司收到的即征即退款项已全额计入“其他收益”。

（2）指定采购的情况下采用总额法确认收入是否符合企业会计准则的规定；

一、企业会计准则相关规定

根据《企业会计准则第 14 号——收入》的相关要求，在判断收入的确认和列报应当采用“总额法”时，一般认为，如果存在以下一种或数种情况，则公司自身被认定为交易的主要责任人，按总额确认收入：

1、根据所签订的合同条款，公司是主要的义务人，负有向客户提供商品或服务的主要责任，包括确保所提供的商品或服务可以被客户接受。

2、公司在交易过程中承担了一般存货风险，即存货所有权上的主要风险和报酬，例如标的商品或服务的价格变动风险、滞销积压风险等。

3、公司能够自主决定所交易的商品和服务的价格，或者自行提供其中的部分服务。

4、公司在向客户提供商品或服务之前，已经从顾客或客户收到全部款项的（即此时公司尚未发生对供应商的付款义务），则公司不承担交易过程中源自顾客或客户的信用风险。

如果不存在上述任一情形，则公司处于代理人地位，按所获取的佣金净额确认收入。如果存在以下情况，可能表明公司处于代理人地位，应按净额法确认收入：根据所签订的合同条款，主要义务人是供应商而不是本公司；公司在交易中

赚取的报酬是事先确定的，或者是固定收益，或者是按确定比例计算；公司不承担信用风险。

二、公司指定采购的情况下采用总额法确认收入符合《企业会计准则》的相关规定

公司所提到的指定采购，为客户对销售合同中的部分产品类进行了指定，但并未指定供应商，公司结合产品要求、供应商价格及交货情况等，自行选取供应商对客户所要求的产品进行采购，出于对《企业会计准则》上述相关规定情形的考虑，公司采用总额法确认收入符合《企业会计准则》相关规定：

（一）公司与客户、供应商分别签订商业合同，合同中均已明确约定了各自的权利及义务

1、公司与客户签订商业合同，对双方的权利和义务进行了明确的约定

公司与客户就项目整体进行谈判，包括项目的功能、项目整体方案、项目的实施进度、项目预估价格、商务条款等，并与客户签订商业合同。在项目的前期谈判接洽中，公司基于客户的实际需求合理预估项目成本。公司综合考虑自身的人员投入情况、外采软件（若有）及硬件的成本、整合工作的复杂度、自主软件利润等情况，向客户出具整体项目的报价（实务中会根据客户的具体要求对报价进行拆分列示）。公司作为合同的主要责任人，负有向客户交付项目并确保项目实现客户预期功能的义务。

2、公司与供应商签订商业合同，对双方的权利和义务进行了明确的约定

公司与客户签订商业合同后，公司根据项目的实际需求情况，在公司的合格供应商名录中选取若干供应商，主要通过招标、询比价、议价谈判等市场化方式进行采购工作。

确定供应商后，公司与供应商签订商业合同，由供应商将相应硬件设备/软件发货至项目实施地（其中部分设备系经过安装公司的软件系统后再发货到项目实施地）或者在项目实施地以公司的名义代表公司向最终客户提供技术服务。在项目的建设过程中，公司全程指派技术人员到现场进行调试或指导的工作，直至完成产品的最终交付。

因此，公司通过招标、询比价、议价等方式，在满足项目实际需求的前提下自主选择确定供应商，并且独立对客户负责，是销售业务的主要责任人。

（二）公司在项目建设过程中承担存货风险

公司承担在建项目中存货所有权上的主要风险和报酬，即商品的价格变动风险、滞销积压风险等。

销售价格系由公司自主向客户投标、报价的方式确定，而供应商的采购价格系公司通过招标、询价、议价等方式确定，公司的采购价格不随客户确认的销售价格的变动而变动。公司承担了该等硬件设备的价格变动风险。

根据采购合同约定，供应商提供的产品/服务经过公司验收确认后，产品/服务正式交付至公司，公司承担了该等产品/服务的相应存货风险，公司需根据合同的相关约定向供应商支付价款。另合同中约定，当供应商提供的产品型号、数量、质量、技术参数等不符合采购合同的约定时，供应商需要承担违约责任，但供应商不对系统的整体联动联调可能产生的损失、无法使用等承担责任。

因此，供应商在采购合同约定的产品/服务的交付后（验收合格），采购合同中的主要义务已履行完毕，产品/服务的主要风险已转移给公司。公司是销售业务的主要责任人。

（三）公司能够自主决定所交易的商品和服务的价格

客户对公司提供的产品/服务明确了技术指标、信息参数、产品品牌等要求，但该类要求未对公司的供应商的选择及采购价格进行限定，公司具有在满足客户要求的前提下，根据项目的实际需求情况，通过招标、询比价、议价谈判等市场化方式进行采购，自主选择供应商及协商供货价格、业务账期的权利。公司在业务实践中，往往先与最终客户沟通合同的整体价格，之后再寻找适当的供应商进行采购。销售价格可由公司根据市场情况自主决定并经由双方协商确定，与公司向上游供应商的采购价格无关。

在采购相应的产品/服务后，公司可以自行决定该产品/服务后续的销售价格、向哪些客户销售等，公司拥有完全的定价权，有权决定客户为取得产品/服务所需支付的价格。因此，相关商品的价格是公司与客户协商、沟通和商业博弈的结果，公司有权自主决定所交易商品的价格，公司是销售业务的主要责任人。

（四）公司承担了信用风险

考虑公司的业务实际情况及对比同一项目下的销售、采购合同中有关收款、付款的条款，公司销售收款进度与采购付款进度无匹配关系。公司根据项目的实

实际需求选择多个不同的供应商，公司根据每个供应商各自的供货进度进行付款。

若确系因供应商提供的商品/服务存在缺陷或者不符合客户的要求而导致客户进行扣款或者索赔时，公司应先行承担赔付责任后，再向供应商追偿。因此，公司承担了该项目中的信用风险，公司是销售业务的主要责任人。

综上，公司单独向客户交付整体的项目产品，就项目整体自主向客户进行报价，同时公司在满足客户整体项目性能的基础上自主选择供应商、自主与供应商约定产品价格，承担供应商交货后的存货风险、客户的信用风险，公司在该交易中的身份为主要责任人。公司指定采购的情况下采用总额法确认收入的依据充分的，符合《企业会计准则》的相关规定。

三、同行业公司收入确认情况

根据同行业可比公司的公开资料，行业内公司同类型产品均采用了总额法确认收入，具体如下所示：

序号	可比公司	收入确认方法	收入确认政策
1	深信服	总额法	(1) 销售商品：在客户取得相关商品控制权的时点，即在按合同约定将产品转移至合同指定地点且签收后确认产品销售收入； (2) 提供劳务：于合同规定的服务期间内分期确认。
2	启明星辰	总额法	(1) 标准化软件产品销售收入：不需要安装调试的标准化产品，在按合同约定将产品的控制权转移给对方后确认销售收入；需要安装调试的标准化产品，按履约进度或按合同约定在项目实施完成并经对方验收合格后确认收入； (2) 客户化软件销售收入：按合同约定在项目实施完成并经对方验收合格后确认收入； (3) 安全服务收入：定期维护服务在服务期间采用直线法确认收入，其他服务按履约进度确认收入；对不属于在某一时段内履行的履约义务，按合同约定在项目实施完成并经对方验收合格后确认收入； (4) 网络安全解决方案：识别为单项履约义务的分别确认，不能识别为单项履约义务的合并作为一项整体履约义务，按履约进度或合同约定在项目实施完成并经对方验收合格后确认收入； (5) 第三方采购销售收入：按合同约定将商品的控制权转移给对方后确认销售收入； (6) 出口销售收入：公司根据销售合同或客户订单要求发出商品，货物报关出口后，凭报关单确认收入。
3	美亚柏科	总额法	(1) 软硬件产品销售合同：产品交付并经客户验收合格后确认收入，分批次交货验收将分批次确认收入； (2) 系统集成类建设合同：项目实施完成并经客户验收合格取得客户签字的验收报告后确认收入； (3) 技术服务合同：按履约进度或在服务成果交付并经客户

			验收通过后确认收入。
4	绿盟科技	总额法	(1) 安全产品收入：客户签收后或在项目实施完成并经对方验收合格后确认收入； (2) 安全服务收入：在项目实施完成并经客户验收合格后或按合同约定在一定服务期内提供服务的项目，在履约期间内分期确认收入。
5	安恒信息	总额法	(1) 不需要实施安装的网络信息安全产品销售收入：按合同约定将产品转移给对方后确认销售收入； (2) 需要实施安装的网络信息安全产品销售收入：合同约定在项目实施完成并经对方验收合格后确认收入； (3) 网络信息安全服务收入：定期维护服务在服务期间采用直线法确认收入，其他服务在经客户验收合格后确认收入； (4) 网络信息安全解决方案：可以分别单独核算的分别确认；不能单独核算的合并核算，并经客户验收合格后确认收入。
6	安博通	总额法	(1) 网络安全产品：将相关产品交付客户后并取得客户签署的收货验收单或对方出具的对账单/系统对账单后确认收入； (2) 技术开发服务：交付服务成果并取得客户签署的验收报告确认收入；安全运维服务，定期取得客户签署的服务工作量确认单后确认收入。
7	山石网科	总额法	(1) 产品销售：按照履约进度、产品转移经客户签收或按合同约定在项目实施完成并经最终用户验收合格后确认收入； (2) 专业服务：维保服务按合同约定期间分期确认；其他专业服务按合同约定在项目实施完成并经客户验收合格后确认收入； (3) 合同或协议内容包括销售商品和提供劳务：能够区分并单独计量的分别处理，不能够区分或单独计量的，在项目整体实施完成并经客户验收合格后确认收入； (4) 销售返利：来自产品销售的货款收入根据公允价值在产品销售收入与返利奖励之间进行分配，与返利奖励相关的部分收入确认为负债，于返利奖励实际使用或失效时结转计入当期损益。
8	奇安信	总额法	(1) 网络安全产品收入：不需要安装调试的安全产品，按合同约定将安全产品转移给对方后确认收入；需要安装调试的安全产品，按合同约定在项目实施完成并经客户验收合格后确认收入； (2) 网络安全服务收入：对于一定服务期内的服务收入，公司按直线法分期确认收入；对于其他服务收入，公司在项目实施完成并取得客户的验收单后确认收入； (3) 硬件及其他收入：可以分别单独核算的分别确认，不能单独核算的合并核算，并经客户验收合格后确认收入。

综上，公司单独向客户交付整体的项目产品，就项目整体自主向客户进行报价，同时公司在满足客户整体项目性能的基础上自主选择供应商、自主决定产品价格，承担供应商交货后的存货风险、客户的信用风险，公司在该交易中的身份为主要责任人。公司指定采购的情况下采用总额法确认收入的依据充分，符合《企业会计准则》的相关规定，且与同行业可比公司收入确认的原则保持一致。

(3) 技术开发委托合同中研究开发经费的资金来源，购置的设备、器材、资料和所有权归属及会计核算情况；

一、技术开发委托合同情况

报告期内公司不存在与研发相关的技术开发委托合同，公司的技术开发委托合同均系与业务项目相关。公司会将非网络靶场技术、攻防类技术等领域的网络安全技术委托第三方开发，并签署《技术开发合同》，其中约定标的技术的内容要求、技术指标、研究开发计划、研究开发经费支付和结算方式等。

研究开发经费是指完成项目研究开发工作需要的成本、报酬是指项目开发成果的使用费和研究人员的科研补贴，该经费的资金来源系公司自有资金，如果研究开发方需要为研究技术购置设备、器材和资料，这部分购置的设备属于完成项目研究开发工作需要的成本，所有权均属于研究开发方。

二、会计核算情况

公司日常账务核算中，主要设置“项目成本”“原材料”“库存商品”科目用以归集公司网络安全产品及服务的成本。“项目成本”按照项目设置项目辅助账，分项目归集各项目实际发生的成本，并设置二级科目“硬件”“人工”“外包”及“其他”。

针对建设项目中涉及的技术开发合同，财务部门按照项目经理提供的阶段验收单的技术开发进度或服务量确认项目成本，计入“项目成本-外包”科目。如技术服务提供完毕，以公司验收报告确认项目成本的完结。

(4) 验收后 1 年的技术驻点服务、成本价升级服务相关的会计核算情况，试用商品的会计核算、收回后的处理机制及财务影响。

一、验收后 1 年的技术驻点服务、成本价升级服务的相关会计核算情况

报告期内，公司与部分客户签订的合同中明确对售后服务期间内提供的额外的附加服务进行了相应的约定，客户一般亦为上述额外的附加服务支付相应的对价并在合同中予以注明。目前合同中约定的“验收后 1 年的技术驻点服务”“成本价升级服务”均属于额外要求公司提供的附加服务。

根据《企业会计准则第 14 号——收入》的相关规定，公司为客户在售后服务期间内提供的额外附加服务构成一项单项履约义务。公司在合同开始日，按照产品销售和额外附加服务两项履约义务的各单独售价的相对比例，将交易价格分

摊至上述两项履约义务中。根据公司的收入确认政策，公司产品销售业务满足合同质量条款的相关约定，客户完成最终验收并签收验收报告后确认其对应的业务收入（根据合同约定拆分后的金额）。额外的附加服务一般为 5*8 驻点服务、成本价升级服务、单独的培训服务等，上述服务一般服务周期为 1-3 年不等，客户在公司提供服务的过程中即取得并消耗公司提供的服务所带来的经济利益，故公司将其确认为某一时段内履行的履约义务，额外的附加服务收入公司一般在整个服务期间内进行分期确认。

报告期内公司合同中含有附加其他履约义务的明细情况如下：

单位：万元

类型	2021 年 1-6 月	收入 占比	2020 年度	收入 占比	2019 年度	收入 占比	2018 年度	收入 占比
运维、驻点服务	157.18	1.93%	55.76	0.16%	6.21	0.04%	33.02	0.18%
VPS、链路服务	189.82	2.33%	27.82	0.10%	2.21	0.01%	-	-
其他服务	24.20	0.30%	33.74	0.12%	21.72	0.13%	12.28	0.07%
合计	371.20	4.56%	117.33	0.37%	30.14	0.18%	45.30	0.25%

公司为客户提供的额外的附加服务类型主要为运维、驻点服务、VPS、链路服务及其他服务，其中运维、驻点服务系公司为客户提供的专业人员驻场技术服务、技术支持服务及系统维护服务费等；VPS、链路服务系 VPS 及隐蔽链路服务等租赁费用，其他服务主要系客户提供的在线学习平台使用权、线下安全培训及实战培训及其他硬件租赁等服务。报告期内合同中含有附加其他履约义务确认收入占各年度分别为 0.25%、0.18%、0.37%和 4.56%。2021 年 1-6 月增长主要由于河池市公安局网络特侦队建设、安全罩总控二期、横云资源采购及研发等项目中客户需求 VPS、链路服务导致的。

二、试用商品的会计核算、收回后的处理机制及财务影响

试用商品系公司应潜在客户要求，免费向其提供的试用设备，所有权属于公司。该试用设备主要用于潜在客户对公司相关产品的性能、运行环境的检验。待客户完成试用后，根据客户的需求情况，公司将其直接销售给客户或者收回试用商品。

（一）试用商品的会计核算、收回后的处理机制

报告期内，公司制定了试用商品的相关管理制度，具体包括：试用商品的申请、试用商品的合同签订、试用商品的出库、试用商品的定期跟踪、试用商品的

回库/销售。

1、试用商品的申请及协议签订

销售部通过与客户洽谈合作机会后提出产品试用申请，申请需经销售经理、销售部门负责人、仓储部门经理、财务总监审批确认；销售员依据审批后的申请，与客户签订《试用协议》。

2、试用商品的出库

销售部人员在《试用协议》签署后，根据协议的相关约定，提出出货申请，仓库部门根据经审批的出货申请单负责试用商品的发货，经客户签收确认的试用单据存放于财务部。财务部门在收到经客户签收确认的试用单据后，建立备查簿登记借出商品并进行账务处理，将借出的试用商品结转至存货-外借存货科目核算。

3、试用商品的定期跟踪

销售部人员每月定期现场查看试用商品的保管及使用情况，确认是否出现质量问题、损毁、丢失等事项。若出现上述事项，及时查明原因，向公司提交相关情况说明。财务部门根据业务人员提交的相关说明对资产状况进行评估，并进行资产处置或者计提资产减值。其中对由客户造成的损失根据《试用协议》一并向客户提出赔偿。

4、试用商品的销售或转回

试用完成后，销售部人员与客户进行沟通确认，了解客户对试用商品的信息反馈，获取购买、继续试用、退回等信息。若客户申请继续试用，销售人员重新执行申请流程，待审批通过后与客户再次签订《试用协议》并向财务部门报备，财务部门更新试用商品备查簿的相关信息；若试用完成后客户购买产品，则销售人员与客户签订销售合同，销售人员向财务部门提交相关说明，财务部门根据该说明更新试用商品备查簿并确认相应的收入，将计入存货-外借存货的产品结转主营业务成本；若试用完成退回，则根据试用协议约定办理退机手续，并将试用商品回库资料提交给财务部门，财务部门更新试用商品备查簿。

仓库人员对于收回的已使用过的旧品，暂时将其单独存放，作为待确定商品进行识别和管理。仓库人员定期会同质量人员、财务人员对已归还待识别的商品进行评估判定，若回收商品经检测后无质量问题，可用于二次出售、研发领用、

固定资产领用，则按照资产原值重新入库存商品。若回收商品经检测后确认无使用价值或者维修成本过高，则予以进行费用化处置，确认为销售费用。

（二）试用商品对财务的影响

报告期内试用商品情况如下：

单位：万元

试用商品类型	2021 年 1-6 月	2020 年	2019 年	2018 年
试用商品金额	129.84	133.84	194.23	137.26
其中：1 年以内	13.76	48.76	158.76	92.96
存货金额	4,464.92	2,953.22	2,417.75	1,475.00
试用商品的占比	2.91%	4.53%	8.03%	9.31%

公司报告期内应客户要求试用的商品金额较小，周期较短，同时公司对借出的商品进行定期跟踪，持续评估其价值并进行相应的财务处理。

【核查程序】

（1）获取发行人收入成本明细表及软件、硬件、服务分类，统计不同业务类别收入情况，分析不同业务类别收入、成本、毛利率波动原因；

（2）访谈发行人财务总监，了解公司软件产品的销售内容、软件产品销售及核算的具体方法，查阅并了解国家相关税收优惠政策，结合公司实际情况，比对公司实际情况与相关税收优惠政策条件的匹配项；

（3）获取报告期内软件产品销售清单，核查申请退税的软件产品与即征即退的税收优惠政策要求的匹配性；获取报告期各期增值税纳税申报表，检查并复核增值税即征即退项目金额与账载金额的一致性；

（4）获取发行人《软件企业认定证书》、《软件产品登记证书》《计算机软件著作权登记证书》等，核查公司相关税收优惠备案情况；核查公司增值税缴纳回单及增值税退税收款回单；查阅增值税即征即退税额申报表及相关申请材料，并与账面记录进行核对，复核软件产品增值税即征即退税额的计算过程；

（5）获取指定采购的项目清单及销售合同，查看合同条款；复核相关项目会计处理；

（6）获取技术开发委托合同清单，查看合同条款；复核相关项目会计处理，核查技术开发委托合同清单资金来源及采购设备的所有权；

(7) 获取销售合同，核查合同履约义务及相关项目会计处理；

(8) 获取报告期内试用产品明细，核查相关内控措施的执行情况；取得试用产品转销明细，核查相关项目会计处理。

【核查意见】

经核查，保荐机构及申报会计师认为：

(1) 发行人软件、服务、硬件收入的具体划分标准系根据合同划分；报告期内发行人主营业务毛利率变动情况合理，报告期内增值税即征即退申报金额及实际收到退税金额与软件产品销售收入间的差异合理，金额具备匹配性；

(2) 发行人指定采购采用总额法确认收入符合企业会计准则的规定；

(3) 发行人技术开发委托合同中的研究开发经费的资金来源为自有资金，合同约定购置的设备、器材、资源和所有权归属受托方；

(4) 验收后 1 年的技术驻点服务、成本价升级服务及试用机相关的会计处理符合企业会计准则的规定，发行人报告期内应客户要求试用的商品金额较小，试用商品对公司整体财务情况影响较小。

8.2、收入季节性

根据申报材料：(1) 报告期各期第四季度收入占比分别为 62.94%、69.54% 和 66.48%；(2) 保荐工作报告中未说明对收入的具体核查情况。

请发行人说明：第四季度各月收入金额及占比情况，2020 年四季度确认收入的主要客户、项目情况，合同签订时间、发货时间、安装调试及验收时间、收入确认时间及依据、回款情况，期后退换货情况及金额。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见，说明对收入的具体核查情况、收入截止性测试的执行情况。

【回复】

请发行人说明：

(1) 第四季度各月收入金额及占比情况，2020 年四季度确认收入的主要客户、项目情况，合同签订时间、发货时间、安装调试及验收时间、收入确认时间及依据、回款情况，期后退换货情况及金额。

一、报告期内公司第四季度收入金额及占比情况

报告期内公司第四季度各月的收入金额及占比情况如下：

单位：万元

期间	2020 年		2019 年		2018 年	
	营业收入	占比	营业收入	占比	营业收入	占比
第四季度	19,577.30	67.13%	9,545.47	58.53%	8,923.90	49.44%
其中：10 月份	1,316.89	4.52%	1,221.95	7.49%	894.71	4.96%
11 月份	1,466.49	5.03%	2,165.34	13.28%	3,303.73	18.30%
12 月份	16,793.92	57.58%	6,158.18	37.76%	4,725.46	26.18%
收入总额	29,164.20		16,308.54		18,051.03	

报告期内公司第四季度收入在当年度收入总额的占比分别为 49.44%、58.53% 和 67.13%，占比较高的主要原因为公司的主要客户的公安等政府部门，该类型客户通常采取预算管理制度和集中采购制度，其采购活动具有较强的季节性。一般在每年上半年进行预算、立项和供应商评定等工作，下半年集中进行采购、签约、施工和验收等工作，从而导致公司第四季度收入占比最高。

二、2020 年四季度确认收入的主要客户、项目情况，合同签订时间、发货时间、安装调试及验收时间、收入确认时间及依据、回款情况，期后退换货情况及金额

单位：万元

序号	客户名称	项目名称	合同金额	第四季度收入确认金额	合同签订时间	发货时间	安装调试时间	验收时间	收入确认时间	依据	截至 2021 年 11 月 30 日的累计回款金额(含税)	回款金额占合同总金额占比
1	郑州高新产业投资集团有限公司	郑州高新区网络空间安全科技馆展陈建筑设计装修布展一体化项目	12,187.50	11,270.09	2020 年 4 月 26 日	2020 年 4 月 30 日至 2020 年 9 月 1 日	2020 年 8 月 2 日至 2020 年 9 月 1 日	2020 年 12 月 25 日	2020 年 12 月	终验报告	11,843.81	97.18%
2	昆山九华电子设备厂	基于网络数据处理技术-评估调度子系统[注 1]	2,486.96	1,886.96	2020 年 7 月 10 日	2020 年 7 月 22 日	2020 年 9 月 20 日至 2020 年 10 月 25 日	2020 年 12 月 1 日至 2020 年 12 月 10 日	2020 年 12 月	终验报告	1,488.26	59.84%
3	公安部十一局	攻防训练资源及培训	862.00	813.21	2020 年 4 月 10 日	2020 年 6 月 10 日至 2020 年 6 月 17 日	2020 年 6 月 17 日至 2020 年 6 月 20 日	2020 年 12 月	2020 年 12 月	终验报告	775.80	90.00%
4	深信服科技股份有限公司	2020 第二届“网鼎杯”网络安全大赛	267.45	251.14	2020 年 4 月 1 日	2020 年 11 月 18 日	2020 年 11 月 20 日	2020 年 11 月 29 日	2020 年 11 月	终验报告	267.45	100%
5	中国信息安全测评中心	数据存储与检索系统	230.00	203.54	2020 年 4 月 22 日	2020 年 5 月 13 日	2020 年 5 月 13 日	2020 年 12 月 9 日	2020 年 12 月	终验报告	230.00	100%
6	成都市互联网信息中心	2020 年“巅峰极客”网络安全技能挑战赛平台服务项目	197.80	186.60	2020 年 8 月 24 日	2020 年 10 月 19 日	2020 年 10 月 24 日	2020 年 12 月 4 日	2020 年 12 月	终验报告	197.80	100%
7	昆明市公安局	网络资源建设项目	189.00	167.26	2019 年 11 月 28 日	2019 年 12 月 2 日	2019 年 12 月 2 日	2020 年 10 月 30 日	2020 年 10 月	终验报告	189.00	100%
8	贵州省公安厅	网络靶场项目	178.00	153.45	2018 年 12 月 17 日	2019 年 8 月 11 日	2019 年 8 月 12 日	2020 年 10 月 25 日	2020 年 10 月	终验报告	178.00	100%
9	大唐高鸿信息技术有限公司	终端及互联网行为监测系统 V1.5、网络数据采集与分析系统 V1.0、网	156.00	138.05	2020 年 12 月 16 日	2020 年 12 月 25 日	2020 年 12 月 25 日	2020 年 12 月 25 日	2020 年 12 月	终验报告	156.00	100%

		络安全态势感知与处置平台 V1.0										
10	广东省公安厅	网络资源支撑服务项目 [注 2]	409.00	129.25	2019 年 11 月 21 日	2019 年 11 月 29 日	2019 年 11 月 29 日	2020 年 11 月 25 日	2020 年 11 月	终验 报告	245.80	60.10%
11	淮安市公安局	网络安全设备采购项目	144.00	127.43	2020 年 3 月 23 日	2020 年 5 月 21 日	2020 年 6 月 3 日	2020 年 12 月 18 日	2020 年 12 月	终验 报告	136.80	95.00%
12	公安部第三研究所	平台软件及硬件设备[注 3]	161.73	125.66	2020 年 12 月 27 日	2020 年 11 月 12 日	2020 年 11 月 12 日 至 2020 年 11 月 13 日	2020 年 12 月 18 日	2020 年 12 月	终验 报告	161.73	100%
13	深圳万佳怡科技有限 公司	e 春秋网络安全实验室靶 场系统 V3.0	140.00	123.89	2020 年 8 月 21 日	2020 年 9 月 27 日	2020 年 11 月 16 日	2020 年 12 月 3 日	2020 年 12 月	终验 报告	140.00	100%
	合计			15,576.53							16,010.45	

[注 1] 昆山九华电子设备厂的基于网络数据处理技术-评估调度子系统项目包括设备供货及运维服务两项履约义务。运维服务自 2021 年 1 月 1 日开始，此处列示设备供货业务的相关收入。截至 2021 年 11 月 30 日，仅考虑设备供货业务的合同额及回款影响，该项目的回款比例为 78.87%。

[注 2] 广东省公安厅的网络资源支撑服务项目根据合同约定分为三个独立子项，2020 年第四季度完成该合同的一个子项。截至 2021 年 11 月 30 日，仅考虑合同约定的子项一对应的合同额及回款影响，子项目一的回款比例为 100.00%。

[注 3] 公安部第三研究所的平台软件及硬件设备项目包括设备供货及运维服务两项履约义务。运维服务自 2021 年 1 月 1 日开始，此处列示设备供货业务的相关收入。

公司 2020 年第四季度收入确认项目存在部分项目验收时间较安装调试时间差异较大，主要原因如下：

1、试运行周期较长

2020 年第四季度确认收入的客户公安部十一局、贵州省公安厅、淮安市公安局等项目，因试运行周期为 6 个月导致验收时间较安装调试时间差异较大。

公司项目验收流程系建设项目在发货到货之后，在客户的项目现场进行安装调试，安装调试完成后，经过系统运行测试后，项目组正式向客户发出验收申请。客户初验小组对项目进行现场验收，检查系统性能，并进行系统功能测试。初验后，公司将软件产品交付客户使用由客户进行试运行，试运行周期一般为 1 至 6 个月，试运行期间并由公司项目人员全程陪同并解决试运行出现的系统问题，客户试运行后，召开验收会并检查项目文档检查，邀请专家评审，终验通过后，完全交付客户使用。

2、疫情影响

2020 年第四季度确认收入的项目中存在因疫情影响导致项目进度放缓，验收工作相比正常进度有所延后。昆明市公安局网络资源建设项目于 2020 年 1 月 9 号初验完成，因疫情影响，导致 1 月至 4 月的试运行中止，试运行周期拉长至 2020 年 10 月完成，最终于 2020 年 10 月完成终验。

3、其他影响验收事项

中国信息安全测评中心数据存储与检索系统项目于 2020 年 5 月 13 日完成产品交付，达到验收条件，但因客户自身验收流程和标准的变动，导致验收时间延迟。

截至 2021 年 11 月 30 日，公司 2020 年四季度确认收入的项目未发生期后退换货的情况。

（2）请保荐机构、申报会计师对上述事项进行核查，并发表明确意见，说明对收入的具体核查情况、收入截止性测试的执行情况。

一、核查程序

1、访谈公司销售负责人，了解公司的销售流程及销售业务的内部控制、公司收入第四季度集中度高的原因，并分析其合理性；

2、取得公司报告期各期分月收入构成情况，核查第四季度收入波动的情况

并分析其合理性；

3、检查公司收入确认依据，检查项目安装调试过程性资料，发货依据、安装调试记录，对于验收时长异常的项目了解其原因，分析原因的合理性；对 2020 年四季度项目的平均验收时长与全年项目的平均验收时长进行比较分析，了解差异的原因，并分析其合理性。

二、核查结论

经核查，保荐机构及申报会计师认为，公司的业务收入存在季节性影响，主要系公司的主要客户为公安等政府部门，该类型客户通常采取预算管理制度和集中采购制度，其采购活动具有较强的季节性。公司各期大体量项目主要集中在四季度进行终验，与行业特性相符，与公司的客户结构相匹配。

三、收入核查的具体情况

（一）保荐机构的核查程序

保荐机构就发行人销售收入执行了以下核查程序：

1、检查报告期各期合同金额大于等于 50 万元项目的中标通知书、销售合同、验收报告等业务资料，并与账面记录核对，进行收入细节测试，确认收入的真实性及真实交易背景。报告期内，经上述细节测试核查金额占主营业务收入的比例分别为 82.57%、82.26%及 90.05%和 88.43%。

2、走访主要客户，通过访谈确认业务背景、交易内容，确认销售业务是否真实发生，从而核查收入的真实性；通过访谈客户，确认项目是否完成，并确认终验情况及终验时间是否准确，进而核查收入是否符合收入确认条件、是否确认至正确的期间。

保荐机构对报告期内客户走访的具体比例如下：

单位：万元

项目	2021 年 1-6 月	2020 年	2019 年	2018 年
走访客户家数	20	31	31	30
走访覆盖收入金额	5,988.59	22,351.50	10,271.16	9,893.31
主营业务收入	8,136.08	29,164.20	16,308.54	18,051.03
走访覆盖收入金额占营业收入比重	73.61%	76.64%	62.98%	54.81%

（1）发行人客户集中度相对较低，客户的地域分布相对分散；

（2）发行人客户结构稳定，主要客户与发行人的合作模式不存在明显变化，

交易不存在异常情况；

(3) 部分客户由于内部管理要求、重大项目或重要任务在施等原因，未配合中介机构执行实地走访程序。

3、对公司主要客户进行函证，函证业务是否发生、收入金额是否准确、函证项目是否经过最终验收及项目的验收时间。将经确认的项目验收时间与收入确认时点进行比对，检查收入是否确认至正确期间。

报告期内，对客户执行的收入函证情况如下：

单位：家、万元

项目	2021年1-6月	2020年	2019年	2018年
发函客户情况				
发函客户家数	58	105	115	158
发函金额	7,698.18	26,346.13	14,823.63	17,626.23
发函金额占当期主营业务收入比例	94.62%	90.34%	90.89%	97.65%
回函客户情况				
回函客户家数	44	85	85	106
回函相符金额	6,264.67	23,084.27	10,326.45	14,178.21
回函相符金额占发函金额比例	81.38%	87.62%	69.66%	80.44%
回函相符金额占当期主营业务收入比例	77.00%	79.15%	63.32%	78.55%
替代性程序验证金额	1,433.52	3,261.87	4,497.18	3,448.02
回函与替代性程序验证金额占当期主营业务收入比例	94.62%	90.34%	90.89%	97.65%
回函与替代性程序验证金额占发函金额的比例	100.00%	100.00%	100.00%	100.00%

报告期内各期，回函相符金额占发函金额比例在 65%以上，占主营业务收入金额比例在 60%以上。针对函证回函不符或未回函部分，保荐机构及申报会计师通过获取相关销售合同、项目实施资料、验收单、发票及收款凭证执行替代测试。2018 年至 2021 年 6 月主营业务收入函证的回函相符金额占发函金额比例相对较低，主要系发行人部分客户未回函造成，而未回函客户主要为政府单位及大型企业，其公章管理严格，内部盖章流程审批较长且复杂，因此回函积极性不强。

(二) 申报会计师的核查程序

1、申报会计师对收入核查的具体情况：

(1) 检查主要项目中标通知书、销售合同、验收报告等业务资料，并与账面记录核对，进行收入细节测试，确认收入的真实性及真实交易背景。报告期内

收入细节测试比例分别为 98.25%、96.67%、99.05%和 100%；

(2) 走访主要客户，通过访谈确认业务背景、交易内容，确认销售业务是否真实发生，现场查看项目是否真实存在，核查收入的真实性；通过访谈确认项目是否完成终验及终验时间，检查收入是否符合收入确认条件、是否确认至恰当的会计期间。

报告期内，申报会计师对客户执行走访程序的情况如下：

单位：家、万元

项目	2021 年 1-6 月	2020 年	2019 年	2018 年
走访客户家数	20	31	31	30
走访覆盖收入金额	5,988.59	22,351.50	10,271.16	9,893.31
主营业务收入	8,136.08	29,164.20	16,308.54	18,051.03
走访覆盖收入金额占营业收入比重	73.61%	76.64%	62.98%	54.81%

(3) 对公司主要客户进行函证，函证业务是否发生、收入金额是否准确、函证项目是否经过最终验收及项目的验收时间。将经确认的项目验收时间与收入确认时点进行比对，检查收入是否确认至恰当的会计期间。

报告期内，对客户执行的收入函证情况如下：

单位：家、万元

项目	2021 年 1-6 月	2020 年	2019 年	2018 年
发函客户情况				
发函客户家数	58	105	115	158
发函金额	7,698.18	26,346.13	14,823.63	17,626.23
发函金额占当期主营业务收入比例	94.62%	90.34%	90.89%	97.65%
回函客户情况				
回函客户家数	44	85	85	106
回函相符金额	6,264.67	23,084.27	10,326.45	14,178.21
回函相符金额占发函金额比例	81.38%	87.62%	69.66%	80.44%
回函相符金额占当期主营业务收入比例	77.00%	79.15%	63.32%	78.55%
替代性程序验证金额	1,433.52	3,261.87	4,497.18	3,448.02
回函与替代性程序验证金额占当期主营业务收入比例	94.62%	90.34%	90.89%	97.65%
回函与替代性程序验证金额占发函金额的比例	100%	100%	100%	100%

四、收入截止性测试的执行情况

对公司收入截止性测试，保荐机构及申报会计师具体执行了如下程序：

（一）保荐机构的核查程序

1、访谈公司销售部门负责人，了解报告期内产品签收、验收过程，是否存在期后销售退回的情形；

2、对主要客户执行函证程序和走访程序，结合回函情况及访谈反馈信息，了解项目的具体验收时间，核查是否存在提前确认收入及延后确认收入的情况；

3、报告期各期末从收入明细账中抽取资产负债表日前后 30 天内随机抽取确认收入的项目，检查上述项目的会计处理凭证、客户验收单据等资料，检查验收单据的时间与账面收入确认时间是否一致；报告期各期末选取验收单据签署日为资产负债表日前后 30 天的随机抽取项目，将上述项目与收入明细账的信息进行核对，检查上述项目是否均已恰当入账，检查上述项目入账时间是否与验收时间保持一致。明细情况如下：

单位：万元

期间	核查金额	占当月收入比例
2021 年 7 月	407.93	81.88%
2021 年 6 月	3,029.89	97.01%
2021 年 1 月	1,192.57	97.94%
2020 年 12 月	15,983.68	95.18%
2020 年 1 月	2,499.33	98.54%
2019 年 12 月	5,347.26	86.83%
2019 年 1 月	138.86	86.40%
2018 年 12 月	4,002.24	83.68%

（二）申报会计师的核查程序

1、访谈公司销售部门负责人，了解报告期内产品签收、验收过程，是否存在期后销售退回的情形；

2、对主要客户执行函证程序和走访程序，结合回函情况及访谈反馈信息，了解项目的具体验收时间，核查是否存在提前确认收入及延后确认收入的情况；

3、报告期各期末从收入明细账中抽取资产负债表日前后 30 天内随机抽取确认收入的项目，检查上述项目的会计处理凭证、客户验收单据等资料，检查验收单据的时间与账面收入确认时间是否一致；报告期各期末选取验收单据签署日为资产负债表日前后 30 天的随机抽取项目，将上述项目与收入明细账的信息进行

核对，检查上述项目是否均已恰当入账，检查上述项目入账时间是否与验收时间保持一致。明细情况如下：

单位：万元

期间	核查金额	占当月收入比例
2021 年 7 月	480.04	91.43%
2021 年 6 月	3,024.78	96.85%
2021 年 1 月	1,138.71	93.52%
2020 年 12 月	16,577.23	98.71%
2020 年 1 月	2,448.78	96.54%
2019 年 12 月	5,999.20	97.42%
2019 年 1 月	139.01	86.49%
2018 年 12 月	4,654.83	98.51%

9、关于期间费用

9.1、销售费用

根据申报材料：报告期各期销售费用中的业务招待费分别为 665.42 万元、652.70 万元和 1,150.40 万元；销售费用中赛事、运营服务费分别为 320.28 万元、224.82 万元和 404.02 万元。

请发行人说明：2020 年业务招待费金额较高的原因，赛事、运营服务费的内容，归集为销售费用未作为项目成本的原因。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见。

请发行人说明：

(1) 2020 年业务招待费金额较高的原因，赛事、运营服务费的内容，归集为销售费用未作为项目成本的原因。

【回复】

一、2020 年业务招待费金额较高的原因

2018 年-2020 各年，公司业务招待费占当期主营业务收入比例均未超过 4%，保持相对稳定。由于公司处于开拓市场、扩展销售渠道的阶段，故业务招待费持续投入。2020 年公司业务规模的不断扩展，业务招待费也相应增长。

2020 年，公司在行业内口碑逐渐提升，技术水平逐渐提高，同时，公司报告期内获得较多的外部投资，资金较为充裕，为进一步在市场竞争中赢得先机，加大了对业务拓展的投入，导致当年业务招待费金额较高。公司业务招待费主要

包括客户拓展、客户维护活动中产生的餐饮费、招待用品费和住宿费等。

报告期内各期，公司承接项目数量、承接项目合同金额、收入确认金额与业务招待费的匹配关系如下：

单位：万元

期间	当期业务招待费	当期主营业务收入	业务招待费占主营业务收入比例
2021 年 1-6 月	697.99	8,136.08	8.58%
2020 年度	1,150.40	29,164.20	3.94%
2019 年度	652.70	16,308.54	4.00%
2018 年度	665.42	18,051.03	3.69%

如上表所示，报告期内各期，业务招待费变动趋势与主营业务收入变动趋势一致，占主营业务收入的比例较为稳定。2020 年业务招待费金额较高的原因系公司加大业务拓展投入，承接项目增加，不存在异常情形。2021 年 1-6 月，业务招待费占主营业务收入比例显著增加，主要原因系随着公司快速发展，项目承揽投入较大。由于收入确认时间较项目承揽时间相对滞后，2021 年 1-6 月业务招待费占主营业务收入比例较往期有所提升。

报告期内，公司承接项目规模及数量的分布情况如下：

单位：个

签约项目的合同金额区间	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
大于 1000 万元	-	5	1	-
500 万元-1000 万元	2	9	8	4
100 万元-500 万元	13	45	43	42
50 万元-100 万元	19	43	51	42
低于 50 万元	66	262	205	253
合计	100	364	308	341

如上表所示，2018 年-2020 年，公司承接项目的分布发生了一定变化，合同金额 100 万元以上的项目数量由 46 个增长到 59 个，增长率为 28.26%。公司逐步加大业务拓展的投入，报告期内承接的体量大、综合性强的项目增加。

2020 年因承接的体量大、综合性强的项目增加，公司业务招待费金额大幅增加，但占主营业务收入比例较为稳定。公司 2020 年业务招待费金额较高主要系公司业务规模扩大。

2021 年，公司加大业务拓展力度，上半年已承接 100 个项目，同时多个项

目尚在跟进中。但由于业务招待费发生时间较合同签订时间更加前置，2021 年 1-6 月合同签订数量和规模与业务招待费支出金额未形成直接匹配关系。

二、赛事、运营服务费的内容，归集为销售费用未作为项目成本的原因

公司赛事、运营服务费分为赛事会务费用支出和销售部门运营支出，服务于公司的业务机会拓展而非项目实施，其在报告期内的金额如下：

单位：万元

项目	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
赛事会务费	32.69	266.17	15.45	51.83
运营服务费	296.90	137.85	209.37	268.45
合计	329.59	404.02	224.82	320.28

报告期内，公司为拓展市场空间，提升口碑及知名度，举办了多项不产生收入的推广性网络安全竞赛，如“红帽杯”网络安全竞赛、全国大学生信息安全竞赛等，以及相关的行业会务支出，如互联网安全责任峰会暨春秋盛典、“粤盾 2020”广东省数字政府网络安全攻防演练活动等。由于推广性网络安全竞赛、行业会务属于公司的业务拓展行为，无法直接为公司带来实质业务收益，故将赛事推广费用确认为销售费用核算。报告期内，公司赛事会务费的金额及构成如下：

单位：万元

项目	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
赛事会务费	32.69	266.17	15.45	51.83
其中：赛事服务费	1.21	15.85	15.45	20.76
会务费	31.48	250.32	-	31.07

报告期内各期，公司举办的推广性网络安全竞赛场次分别为 25 场，17 场及 14 场和 3 场，与赛事服务费变动趋势不存在重大差异。2020 年公司会务费支出金额较大，原因系公司为响应行业政策，提升行业影响力，参与举办了“粤盾 2020”广东省数字政府网络安全攻防演练活动，在该活动中担任主要承办方和主要技术支持单位。

运营服务费支出主要包括于未形成收入项目的前期投入、协会会费等。由于上述费用的投入无法直接为公司带来实质的业务收益，故将运营服务费用确认为销售费用核算。报告期内，公司运营服务费的构成如下：

单位：万元

项目	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
----	--------------	---------	---------	---------

运营服务费	296.90	137.85	209.37	268.45
其中：未形成收入项目前期投入	261.12	92.50	189.69	202.78
协会会费	0.50	14.41	18.71	6.75
其他运营支出	35.28	30.94	0.97	58.93

报告期内各期，公司运营服务费支出主要集中于未形成收入项目前期投入，相关支出为公司在业务拓展中的必要支出。协会会费支出及其他运营支出分别为公司在维护资质、销售部门运营中形成的支出，相关行为服务于公司销售活动。

在核算方面，赛事、运营服务费中的项目前期投入与存货中的项目成本有效区分。对于部分尚未签订合同但项目的非标准化程度和复杂程度较高的项目，公司响应客户实际需求，提前以现场沟通、开展技术试点等方式参与项目部署。同时，销售部门项目负责人根据未签订项目合同的实际执行情况持续与客户进行沟通。每个月项目经理将沟通结果通报销售部门经理，销售部门经理根据实际情况判断预计签订合同的可能性，将暂未签订的合同进行分类，分别系“预计可以签订合同”和“无法签订合同”项目，并将信息通报公司产销运营管理中心和财务部门，财务部门将“无法签订合同”的项目成本计入“销售费用-赛事、运营服务费”。

对于“预计可以签订合同”的项目，公司在持续跟进项目的过程中编制《项目执行情况表》，结合相关项目属于前期项目的延伸和项目实施人员持续参与客户相关服务等判断合同签订的可行性。截至 2021 年 12 月 20 日，公司报告期各期末计入存货的项目成本中，已签订合同项目的项目成本账面余额占比分别为 100%、97.94%、100%和 98.78%。其中，2019 年末在施项目中，最终未签订合同的项目共计 3 个，其 2019 年末项目成本账面余额合计为 40.83 万元，公司在 2020 年确认相关合同无法签订时，将相应金额计入销售费用。公司存货中的项目成本核算准确，有效区分于赛事、运营服务费。

综上所述，公司赛事、运营服务费支出服务于公司销售活动，不直接形成收入，故归集为销售费用而非项目成本具有合理性。

【核查程序】

1、获取发行人报告期内合同台账，核查报告期内发行人项目承接数量及规模与业务招待费的匹配关系；

2、发行人访谈总经理、财务总监,了解 2020 年业务招待费金额较高的原因,了解赛事、运营服务费中项目前期投入与存货的核算区分方式;

3、获取发行人业务招待费有关的规定以及业务招待费用明细,并采用抽样方式检查相关的发票、付款等单据,检查业务招待费是否真实、准确;

4、获取发行人赛事、运营服务费明细表,核查其形成原因及主要构成;

5、获取发行人举办的网络赛事立项、运营服务等对应资料,检查相关合同等单据,核查赛事、运营服务费的归集是否完整准确,并结合对发行人销售部门的访谈,了解赛事、运营服务费的形成原因。

【核查意见】

经核查,保荐机构和申报会计师认为:

1、报告期各期,公司业务招待费与当期承接项目数量具备匹配关系,且占主营业务收入比例稳定,2020 年业务招待费金额较高主要系公司加大业务拓展所致;

2、公司赛事、运营服务费属于业务拓展过程中的支出,计入销售费用而非项目成本具备合理性。

9.2、研发费用

根据申报材料:(1)报告期内研发人员职工薪酬逐年下降,研发费用对应的研发项目均已完成;(2)定制软件产品开发时公司会组织研发团队开展工作;

(3)报告期各期折旧费分别为 218.10 万元、175.36 万元和 788.31 万元,2020 年金额较大主要是由于北京市工程实验室于 2019 年 12 月完工转固,2020 年 1 月开始计提折旧。

请发行人说明:(1)研发人员职工薪酬逐年下降的原因,人均薪酬是否与当地薪酬水平相匹配,结合研发项目、研发人员及其薪酬变化情况说明研发的可持续性;(2)定制软件产品开发支出作为研发费用/项目成本的核算依据、核算金额;(3)北京市工程实验室的用途,相关折旧费在成本/费用中的摊销情况。

请保荐机构、申报会计师对上述事项进行核查,并发表明确意见。

请发行人说明:

(1)研发人员职工薪酬逐年下降的原因,人均薪酬是否与当地薪酬水平相匹配,结合研发项目、研发人员及其薪酬变化情况说明研发的可持续性;

【回复】

一、研发人员职工薪酬逐年下降的原因

报告期内，公司研发人员主要参与研发工作，也在必要时参与项目工作，为项目实施提供技术支持。公司将研发人员的薪酬支出根据其从事的研发活动和项目实施活动工时申报情况，分别计入研发费用和项目成本。因此，报告期内研发费用中的职工薪酬系根据研发人员实际参与研发活动的工时数据计算。为保证研发人员填报工时的准确性，公司制定了完善的内控流程，且通过工时系统进行控制。

2018 年，计入研发费用的研发人员薪酬较高，主要原因系公司研发人员数量较多，研发活动较为集中，并在当期形成了较多知识产权。研发人员当期在研发项目中的工时投入亦较为集中。

2019 年，计入研发费用的研发人员薪酬较 2018 年有所降低，主要原因是 2019 年初公司搬迁到新的办公场所，2019 年部分研发人员离职，致使研发人员数量较 2018 年有所减少，研发人员薪酬总额较 2018 年有所降低。

2020 年，由于公司承接项目的数量和规模增加，更多研发人员为项目实施提供必要的技术支持，研发人员在研发项目中的工时投入有所降低，致使计入研发费用的研发人员薪酬降低。此外，受疫情期间社保减免政策影响，2020 年研发人员薪酬总额较 2019 年亦存在小幅降低。

2021 年 1-6 月，由于计入研发费用的研发人员薪酬为半年度薪酬，故计入研发费用的薪酬总额较 2018 年-2020 年偏低。

综上所述，报告期内，计入研发费用的研发人员薪酬逐年下降主要受研发人员在研发项目中的实际工时投入影响以及研发人员数量影响，计入研发费用的研发人员薪酬变动情况与公司实际经营背景相匹配，不存在异常。

二、研发人员人均薪酬水平

报告期内，研发人员薪酬总额及各年度研发人员平均薪酬具体如下：

单位：万元

期间	研发人员平均数量	研发人员薪酬合计	平均年度薪酬
2021 年 1-6 月	174	2,370.76	27.25
2020 年度	145	3,679.22	25.30
2019 年度	145	3,890.08	26.86

2018 年度	210	5,068.40	24.12
---------	-----	----------	-------

注 1：报告期各期，研发人员平均数量=各月研发人员数量之和/12；2020 年平均薪酬受社保减免影响。

注 2：2021 年 1-6 月平均薪酬为年化平均薪酬，年化薪酬=半年度平均薪酬*2，未包含全年奖金计提。

如上表所示，按研发支出口径将计入研发费用及项目成本的研发人员薪酬合并计算，报告期内研发人员平均薪酬无重大波动。

报告期内公司的奖金计提政策、研发人员入职和离职等因素，对公司的研发人员平均薪酬的变动产生一定影响，公司报告期内研发人员平均薪酬无重大波动。2019 年研发人员平均薪酬较 2018 年有所上升，主要原因系当期部分研发人员由于个人、办公场所搬迁等原因离职，而稳定在职的研发人员主要为工作时间较长，工作经验充足的员工，该类员工平均薪酬较高，致使 2019 年研发人员平均薪酬较 2018 年有所增长。2020 年，受新冠疫情期间社保减免等因素影响，研发人员平均薪酬较 2019 年小幅降低。2021 年 1-6 月平均年化薪酬高于 2018 年-2020 年各年度平均薪酬，主要原因系公司进一步加强了研发人员薪酬待遇。2020 年，研发人员涉及社保减免金额约 598.37 万元，如将该金额还原至研发人员薪酬，则报告期内研发人员薪酬变动情况如下：

期间	研发人员平均数量	研发人员薪酬合计	平均年度薪酬
2021 年 1-6 月	174	2,370.76	27.25
2020 年度	145	4,277.59	29.42
2019 年度	145	3,890.08	26.86
2018 年度	210	5,068.40	24.12

如将社保减免金额还原至研发人员薪酬，则 2018 年至 2020 年公司研发人员平均薪酬逐年上升。

综上所述，报告期内公司注重研发投入，持续提高研发人员薪酬水平，研发人员平均薪酬总体稳定，平均薪酬变动情况存在合理背景。

三、与当地市场薪酬水平对比情况

由于公司属于软件和信息技术服务业企业，研发人员集中于北京市，因此选取北京市信息传输、软件和信息技术服务业平均薪酬进行比较。报告期内，公司研发人员人均薪酬与当地市场薪酬水平比较情况如下：

单位：万元

项目	2021年1-6月	2020年度	2019年度	2018年度
公司研发人员平均薪酬	27.25	25.30	26.86	24.12
北京市信息传输、软件和信息技术服务业平均薪酬	未公示	22.88	23.61	20.58

注：北京市信息传输、软件和信息技术服务业平均薪酬来源于北京市统计局公示信息。

公司为聚焦科技创新的网络安全企业，注重研发投入和技术开发。报告期内，公司研发人员平均薪酬高于北京市信息传输、软件和信息技术服务业平均薪酬，具有合理性。

四、研发可持续性

报告期内，公司核心技术团队、研发人员数量及研发人员薪酬相对稳定，研发项目持续形成研发成果，公司研发具备可持续性，具体如下：

项目	2021年1-6月 /2021.6.30	2020年度 /2020.12.31	2019年度 /2019.12.31	2018年度 /2018.12.31
研发项目数量	12	13	14	12
核心技术人员数量	9	9	9	8
当期开发完成的软件著作权数量	15	23	17	29
期末研发人员占比	45.94%	43.44%	44.01%	53.75%
研发人员年化平均薪酬(万元)	27.25	25.30	26.86	24.12

如上表所示，报告期内公司在研发领域持续投入，保持核心技术团队及研发人员的稳定性，研发活动持续申请或形成知识产权。此外，公司重视研发的基础设施投入和人员激励，建设并使用服务于研发的北京市工程实验室，建立了完整的研发体系，重视核心技术人员及研发人员激励。截至本回复出具之日，公司核心技术人员均通过信安春秋持有公司股份，公司亦在《科研成果管理制度》中规定了对科研成果贡献和申报专利的奖励制度。综上所述，公司研发具备可持续性。

(2)定制软件产品开发支出作为研发费用/项目成本的核算依据、核算金额；

一、研发人员的工作职能

公司的研发人员就职于公司设立的研发部门，主要工作包括技术和产品的开发、维护、升级等。在研发方面，研发人员根据市场中的热点方向及市场需求，基于技术的可行性，研究开发标准化软件产品或技术，公司核心技术据此形成基础架构。

在项目实施方面，公司会根据客户实际需求开发定制化软件。由于定制化软

件开发对行业经验、专业能力要求较高，因此会由研发人员参与，以提供技术支持，保证交付质量。报告期内，公司定制化软件产品开发基于客户需求，服务于项目实施。

公司对研发人员的职能划分符合同行业可比上市公司惯例，具体如下：

公司名称	人员类别	工作职能
启明星辰	科研技术人员	负责技术研究和产品开发
美亚柏科	研发和技术人员	负责公司产品的研发、测试、管理及维护，为客户提供软件产品和解决方案等
绿盟科技	研发与技术人员	负责技术研究，为产品开发和工程服务部门提供技术支撑
深信服	研发人员	主要负责研发平台、前沿基础技术的研究和预研等，有专人专岗接触客户并了解客户诉求
安恒信息	研发人员	负责技术研究，并为产品开发和工程服务部门提供技术支撑
安博通	研发人员	负责标准化技术和标准化软件的研究和开发
山石网科	产品研发人员	负责技术与软硬件开发
奇安信	研发人员	参与产品、技术平台相关技术预研、可行性研究、产品和解决方案设计、开发与验等，也直接向客户提供安全服务与产品解决方案
永信至诚	研发和技术人员	负责技术和产品的开发、维护、升级等，也根据项目的定制化需求参与项目实施

注：同行业可比上市公司人员类别及职能划分取自同行业可比上市公司的招股说明书。

如上表所示，同行业可比上市公司研发人员的职能亦不完全局限于产品或技术的开发，也存在根据实际需要参与服务客户的情况。公司研发人员在必要时参与项目实施的情况符合行业惯例，有助于充分发挥人效，提升公司产品和服务质量。

二、参与定制化开发项目的成本支出的核算依据、核算金额

（一）参与定制化开发项目的成本支出的核算依据

公司制定了《费用支出核算办法》，规定将研发人员当期的职工薪酬及相关费用纳入研发支出科目进行归集和核算，根据实际情况将研发支出分配为研发费用和项目成本。研发人员根据实际需求参与定制化开发项目时，由研发人员在系统中填报定制化开发项目的实际工时。公司每月根据填报并经审批的工时计算、分配参与定制化开发项目的实际人工成本，由相应的研发支出科目转入项目成本中核算。为保证研发人员填报工时的准确性，公司制定了完善的内控流程，且通过工时管理系统进行控制。

（二）定制化开发项目的成本支出的核算金额

报告期内，公司定制化软件开发支出由研发支出结转至项目成本，研发支出在研发费用及项目成本中的归集情况如下：

单位：万元

项目	2021 年 1-6 月	2020 年度	2019 年度	2018 年度
研发支出	2,937.30	4,904.09	4,361.21	5,503.40
其中，转入相应成本费用的金额如下：				
研发费用	2,560.74	3,847.85	3,544.59	4,347.00
项目成本	376.56	1,056.24	816.62	1,156.40

报告期内，公司基于客户要求的定制化软件开发支出已计入相应的项目成本中，公司不存在将定制化产品的开发支出计入研发费用的情况。

三、北京市工程实验室的用途，相关折旧费在成本/费用中的摊销情况

根据北京市人民政府《关于印发<北京市工程研究中心管理办法>和<北京市工程实验室管理办法>的通知》（京发改〔2010〕652 号），工程实验室是依托企业、转制科研机构、科研院所或高校等设立的研究开发实体，是北京市创新体系的重要组成部分。公司建设的网络安全空间智能仿真和众测关键技术与服务北京市工程实验室（以下简称“工程实验室”）是经北京市发改委认定的 2017 年 49 家工程实验室之一。

工程实验室于 2017 年 1 月实际开始建设，实际建设周期为 2017 年 1 月至 2019 年 12 月。2019 年 12 月达到预计可使用状态转固，次月及 2020 年 1 月开始计提折旧。2020 年 6 月，北京中珊会计师事务所出具了工程实验室项目专项审计报告，工程实验室项目于 2020 年 10 月取得了北京市海淀区发展改革委员会的验收批复。

工程实验室的建设目标紧密围绕网络空间安全智能仿真和众测领域，旨在通过研发手段，开展关键核心技术的试验研究以及融合战略性和前瞻性技术研发。工程实验室通过搭建网络空间安全平行仿真和众测的技术支持平台，来增强公司在网络空间安全平行仿真技术和对网络安全关键领域的支撑保障能力，促使公司为互联网安全、网络靶场、众测领域等的产业发展提供更加完善的技术支持。

在应用方面，工程实验室由研发部门负责运行，主要围绕以下方面：

1、作为功能完善的基础设施平台，为公司的技术开发活动提供计算资源、网络资源和实验资源；

2、依托基础设施，沉淀和留存公司的项目经验和行业经验，持续构建用于提升技术能力的数据库；

3、实现公司核心技术的突破，打造自主创新与产学研相结合的开放式创新体系，积极承担国家、地方的科研项目，为网络安全行业提供高素质后备人才。

综上所述，工程实验室的运行是基于研发目的，具备研发属性。报告期内，工程实验室于 2020 年 1 月开始计提折旧，固定资产折旧全部计入研发费用，2020 年当期计提的折旧金额为 642.45 万元，2021 年 1-6 月计提的折旧金额为 321.23 万元。

【核查程序】

1、获取发行人关于研发支出归集、工时填报的相关制度，评价这些控制的设计，确定其是否得到执行，并测试相关内部控制的运行有效性；

2、访谈研发负责人及财务总监，了解公司研发人员的工作内容、工时分配方法及工时分配依据；

3、获取报告期内发行人研发人员工时统计表，核查研发人员报告期内的工时分配及变动情况，抽取样本对工时分配情况进行重新计算；

4、获取发行人研发支出明细表及研发人员工资表，核查研发人员的数量变动情况、薪酬总额及人均薪酬变动情况；

5、在北京市统计局网站查询当地信息传输、软件和信息技术服务业平均薪酬，并分年度与发行人研发人员平均薪酬进行比对分析；

6、获取发行人研发项目情况表、研发人员清单、报告期内软件著作权清单，分析研发项目、研发人员、核心技术人员、软件著作权的匹配性；获取发行人《科研成果管理制度》及股权激励的人员名册，了解核心技术人员和研发人员的激励情况；

7、访谈总经理及财务总监，了解定制化软件开发的用途以及相应开发支出的核算依据；检查定制化软件开发项目的会计核算资料，检查定制化软件开发项目的分配是否恰当、准确；

8、访谈研发负责人，了解工程实验室的建设背景和实际用途；

9、获取发行人的研发费用明细表，核查报告期内工程实验室折旧的归集情况。

【核查意见】

经核查，保荐机构及申报会计师认为：

1、报告期内，公司计入研发费用的研发人员薪酬总额存在波动的主要原因系研发人员薪酬根据实际研发工时核算，计入研发费用的研发人员薪酬总额与项目工时的变动趋势一致；

2、报告期内，公司研发人员平均薪酬较为稳定，薪酬变动存在合理背景，与当地市场平均薪酬不存在重大差异；

3、公司根据客户需求进行定制化软件开发，相应开发支出计入项目成本，不存在计入研发费用的情形，公司研发人员参与项目实施具备必要性，符合行业惯例；

4、北京市工程实验室的建设、使用基于研发目的，其固定资产折旧计入研发费用具有合理性。

10、关于应收账款

根据申报材料：（1）报告期各期应收账款账面原值分别为 10,451.18 万元、10,978.56 万元和 9,997.65 万元；（2）2020 年账龄为 2-3 年、3-4 年的应收账款占比分别为 18.16%、5.42%，较 2019 年大幅上升；（3）截至 2021 年 6 月 22 日的期后回款比例分别为 71.82%、61.57%和 47.43%。

请发行人说明：期后回款比例较低的原因，是否存在逾期的应收账款、对应的主要客户情况及逾期的原因，2020 年账龄为 2-3 年、3-4 年的应收账款占比大幅上升的原因。

请保荐机构、申报会计师对上述事项进行核查，说明对报告期各期末应收账款的核查情况。

【回复】

请发行人说明：

（1）期后回款比例较低的原因，是否存在逾期的应收账款、对应的主要客户情况及逾期的原因，2020 年账龄为 2-3 年、3-4 年的应收账款占比大幅上升的原因。

一、最新期后回款比例及期后回款比例较低的原因

截至 2021 年 11 月 30 日，公司报告期各期末应收账款期后回款比例分别为 76.78%、70.36%、63.52%和 40.09%，回款比例较低主要受以下方面影响：

（一）客户审批流程复杂，付款周期较长：

公司客户及最终用户多为政府单位（包括公安机关和其他政府单位）和军队，内部审批流程较为复杂，付款周期较长。在达到合同约定的付款节点后，客户通常还需要进行项目资料审核，并结合资金预算办理内部审批、申请付款等一系列手续，导致公司收款时间存在延后情形，收回款项进度较慢。

（二）新冠疫情及相关政策影响

受 2020 年新冠疫情影响，公司客户的付款进度普遍有所推迟，加之 2021 年疫情防控常态化趋势下地方政府财政预算政策普遍有所调整，公司政府单位客户付款流程的实际执行受政府预算管理政策约束，部分政府单位客户虽已提交付款流程，但实际付款节点仍基于政府预算政策受各地方政府统一管理。

（三）客户付款节点相对固定：

政府单位为公司的主要客户群体，而地方政府机关受财政预算影响，结算付款时间相对固定且主要集中在第四季度，因此公司 2020 年末应收账款期后回款比例较低。

（四）质保金及异常客户影响：

公司与客户签订的销售合同中约定了质保金的金额及到期时间，质保金到期时间较项目验收时间明显延后。2020 年末，公司按照新收入准则将质保金归集至合同资产科目，但 2018 年末及 2019 年末的应收账款账面余额包含合同约定的质保金。截至 2021 年 11 月 30 日，2018 年末及 2019 年末的部分质保金尚未到期，拉低了 2018 年末及 2019 年末的期后回款比例。

此外，由于公司部分客户资金紧张，导致报告期各期末部分款项预计无法收回，公司已对该等应收账款单项计提了坏账准备。而应收账款期后回款的计算以应收账款的账面余额为依据，该等应收账款账面余额长期无法收回，拉低了期后回款比例。截至 2021 年 6 月 30 日已单项计提坏账准备的应收账款债务人报告期各期末的应收账款账面余额分别为 605.35 万元、605.35 万元、605.35 万元和 599.02 万元。

如将 2018 年末及 2019 年末应收账款账面余额剔除截至 2021 年 11 月 30 日尚未到期的质保金及截至 2021 年 6 月 30 日已单项计提坏账准备部分,则公司期后回款比例如下:

单位: 万元

时间	尚未到期的质保金和已单项计提坏账准备金额合计	剔除质保金和单项计提影响后的期后回款比例
2021 年 6 月 30 日	599.02	46.67%
2020 年 12 月 31 日	605.35	69.57%
2019 年 12 月 31 日	711.83	76.84%
2018 年 12 月 31 日	610.29	82.62%

如上表所示,剔除尚未到期质保金及坏账影响后,公司报告期各期末应收账款期后回款比例均有所提升。

公司应收账款周转情况总体符合行业惯例,公司 2020 年末及 2021 年 6 月末账龄 1 年以上的应收账款占比与同行业可比上市公司的具体比较如下:

时间	公司名称	账龄 1 年以上应收账款账面余额占应收账款账面余额比例
2021 年 6 月 30 日	启明星辰	36.47%
	美亚柏科	45.38%
	绿盟科技	52.48%
	深信服	11.49%
	安恒信息	15.49%
	安博通	37.59%
	山石网科	31.08%
	奇安信	19.47%
	发行人	46.95%
	同行业可比上市公司平均	31.18%
2020 年 12 月 31 日	启明星辰	37.54%
	美亚柏科	38.24%
	绿盟科技	38.45%
	深信服	8.78%
	安恒信息	14.36%
	安博通	46.64%
	山石网科	35.38%
	奇安信	20.26%

	发行人	39.85%
	同行业可比上市公司平均	29.96%

如上表所示，公司应收账款周转总体良好，同行业可比上市公司中，部分公司存在应收账款账龄结构与发行人相近的情况，2020 年末及 2021 年 6 月末账龄一年以上的应收账款占账面余额比例与同行业可比上市公司不存在重大差异。

上表中，启明星辰、美亚柏科、绿盟科技和安博通账龄 1 年以上应收账款占比与公司差异较小，应收账款流动性与公司总体接近。主要原因系上述同行业可比上市公司业务模式与公司接近。在业务模式方面，公司与启明星辰、美亚柏科、绿盟科技和安博通主要产品和服务的非标准化程度普遍较高，使得结算周期较长。

公司 2020 年末及 2021 年 6 月末账龄 1 年以上的应收账款占比高于深信服、安恒信息、山石网科和奇安信主要受业务模式及结算方式影响。深信服、安恒信息、山石网科及奇安信产品的标准化程度更高，相较于启明星辰、美亚柏科、绿盟科技、安博通及发行人，销售模式更加侧重于渠道销售，结算周期更短，致使应收账款流动性较强，其在渠道销售体系下的结算方式主要如下：

公司名称	渠道销售模式下的结算特点
深信服	渠道代理模式收入占比较高，在结算方式上主要采取预收款的形式，导致预收账款金额较高，应收账款规模较小，应收账款周转率较高。
山石网科	在渠道销售模式下，主要采用先款后货的结算方式。
安恒信息	渠道销售模式下，采用预付款政策的销售收入占比较高。预付货款的比例一般为 30%、50%，以 50%为主。
奇安信	在渠道销售模式下，对于行业经销商群体，原则上要求 100%预付款。

如上表所示，应收账款账龄结构优于发行人的同行业上市公司得益于渠道销售体系下向代理商收取预收款项，使得结算周期较短，应收账款规模较小，应收账款流动性更强。如剔除上述四家同行业可比上市公司，则公司账龄 1 年以上应收账款占比与其他同行业可比上市公司的差异如下：

时间	公司名称	账龄 1 年以上应收账款账面余额占应收账款账面余额比例
2021 年 6 月 30 日	启明星辰	36.47%
	美亚柏科	45.38%
	绿盟科技	52.48%
	安博通	37.59%
	发行人	46.95%

	同行业可比上市公司平均	42.98%
2020 年 12 月 31 日	启明星辰	37.54%
	美亚柏科	38.24%
	绿盟科技	38.45%
	安博通	46.64%
	发行人	39.85%
	同行业可比上市公司平均	40.22%

如上表所示，2020 年末及 2021 年 6 月末，公司账龄 1 年以上应收账款账面余额占比与启明星辰、美亚柏科、绿盟科技、安博通及其平均值接近。剔除产品类型、结算模式与发行人差异较大的深信服、安恒信息、山石网科及奇安信后，公司与账龄 1 年以上应收账款账面余额占比与其他同行业可比上市公司较为接近。

二、逾期应收账款及 2020 年长账龄应收账款情况

（一）逾期应收账款

报告期内，公司逾期应收账款情况如下：

单位：万元

项目	2021 年 6 月末		2020 年末		2019 年末		2018 年末	
	金额	占比	金额	占比	金额	占比	金额	占比
应收账款 账面余额	9,101.08	100%	9,997.65	100%	10,978.56	100%	10,451.18	100%
逾期金额	6,887.68	75.68%	5,614.11	56.15%	6,971.54	63.50%	6,964.11	66.63%
其中：逾期 1 年以内	3,222.62	35.41%	1,940.73	19.41%	4,110.92	37.45%	4,767.84	45.62%
逾期 1 年 以上	3,665.06	40.27%	3,673.38	36.74%	2,860.61	26.06%	2,196.27	21.01%

公司逾期应收账款依照合同约定计算。由于公司与客户签订的合同一般未约定信用期，仅约定付款节点。而公司客户以政府单位、军队为主，上述客户付款审批流程较长，实际付款节点难以与合同约定完全匹配，导致公司部分应收账款在项目验收及收入确认后，短期内即形成逾期情况。报告期各期末，公司逾期应收账款对应的主要客户、逾期金额、逾期原因、坏账准备计提情况及期后回款情况如下：

1、2021 年 6 月 30 日逾期应收账款

序	客户名称	逾期	逾期部	逾期部	逾期原因	逾期部分截至
---	------	----	-----	-----	------	--------

号		金额	分坏账 准备金 额	分期后 回款金 额		2021年11月30 日回款比例
1	网神信息技术(北京)股份有限公司	498.76	24.94	498.76	受内部安排影响,付款审批进度推迟	100.00%
2	郑州高新产业投资集团有限公司	481.80	24.09	481.80	受内部安排影响,付款审批进度推迟	100.00%
3	北京华威益腾通讯技术有限公司	441.10	109.87	441.10	该客户未将最终用户款项收回完毕,故未相应支付给公司	100.00%
4	安溪县公安局	384.99	192.49	0.00	受政府财政预算影响,付款审批进度推迟	0.00%
5	贺州市公安局	350.00	175.00	0.00	受政府财政预算影响,付款审批进度推迟	0.00%
6	大田县公安局	314.47	15.72	0.00	受政府财政预算影响,付款审批进度推迟	0.00%
7	乌鲁木齐市公安局	294.80	68.54	0.00	受政府预算影响,付款审批进度推迟	0.00%
8	中海油信息科技有限公司北京分公司	262.80	13.14	262.80	受内部安排影响,付款审批进度推迟	100.00%
9	厦门安胜网络科技有限公司	258.00	12.90	0.00	该客户未收到最终用户款项,故未相应支付给公司	0.00%
10	成都天用唯勤科技股份有限公司	224.00	11.20	224.00	受内部安排影响,付款审批进度推迟	100.00%
11	南京市公安局	218.74	65.62	218.74	受政府财政预算影响,付款审批进度推迟	100.00%
12	北京神州泰岳教育科技有限公司	209.00	209.00	0.00	2020年已确认为坏账并全额计提坏账准备	0.00%
13	天津光电通信技术有限公司	184.21	9.21	0.00	受内部安排影响,付款审批进度推迟	0.00%
14	广西戴亚柯仑信息科技有限公司	162.00	16.20	0.00	该客户未收到最终用户款项,故未相应支付给公司	0.00%
15	中国人民解放军	160.72	16.07	149.24	受单位安排影响,付款审批进度推迟	92.86%
16	上海安询信息技术有限公司	155.40	15.54	0.00	最终用户款项尚未收回完毕	0.00%

17	公安部十一局	142.06	14.21	0.00	受政府财政预算影响，付款审批进度推迟	0.00%
18	湖南雨人网络安全技术股份有限公司	140.00	42.00	0.00	最终用户款项尚未收回完毕	0.00%
19	武夷山市公安局	119.33	59.66	0.00	受政府财政预算影响，付款审批进度推迟	0.00%
20	中国电子信息产业集团有限公司第六研究所	103.50	5.18	49.50	受新冠疫情及单位安排等原因影响，付款审批进度推迟	47.83%
合计		5,105.67	1,100.58	2,325.94	-	45.56%

2、2020 年 12 月 31 日逾期应收账款

单位：万元

序号	客户名称	逾期金额	逾期部分坏账准备金额	逾期部分分期后回款金额	逾期原因	逾期部分截至 2021 年 11 月 30 日回款比例
1	昆山九华电子设备厂	630.00	31.50	630.00	受政府财政预算影响，付款审批进度推迟	100%
2	北京华威益腾通讯技术有限公司	441.10	109.87	441.10	该客户未收到最终用户款项，故未相应支付给公司	100%
3	安溪县公安局	384.99	115.50	-	受政府财政预算影响，付款审批进度推迟	-
4	山西省公安厅	302.40	15.12	302.40	受政府财政预算影响，付款审批进度推迟	100%
5	乌鲁木齐市公安局	294.80	68.54	-	受新疆疫情影响，付款审批进度推迟	-
6	贺州市公安局	250.00	75.00	-	受政府财政预算影响，付款审批进度推迟	-
7	南京市公安局	218.74	65.62	218.74	受政府财政预算影响，付款审批进度推迟	100%
8	北京神州泰岳教育科技有限公司	209.00	209.00	-	2020 年已确认为坏账并全额计提坏账准备	-
9	上海安询信息技术有	174.90	16.52	19.50	最终用户款项尚未	11.15%

	限公司				收回完毕	
10	广西戴亚柯仑信息科技有限责任公司	162.00	16.20	-	该客户未收到最终用户款项,故未相应支付给公司	-
11	中国人民解放军	160.72	16.07	149.24	受单位安排影响,付款审批进度推迟	92.86%
12	公安部十一局	142.06	14.21	-	受政府财政预算影响,付款审批进度推迟	-
13	深圳万佳怡科技有限公司	140.00	7.00	140.00	该客户未收到最终用户款项,故未相应支付给公司	100%
14	湖南雨人网络安全技术股份有限公司	140.00	42.00	-	客户未收到最终用户款项,故未相应支付给公司	-
15	南京烽火星空通信发展有限公司	135.10	40.53	135.10	客户未收到最终用户款项,故未相应支付给公司	100%
16	武夷山市公安局	119.33	59.66	-	受政府财政预算影响,付款审批进度推迟	-
合计		3,905.14	902.33	2,036.08	-	52.14%

3、2019年12月31日逾期应收账款

单位：万元

序号	客户名称	逾期金额	逾期部分坏账准备金额	逾期部分分期后回款金额	逾期原因	逾期部分截至2021年11月30日回款比例
1	南京市公安局	770.00	77.00	770.00	受政府财政预算影响,付款审批进度推迟	100%
2	北京华威益腾通讯技术有限公司	709.10	76.56	709.10	最终用户款项尚未收回完毕	100%
3	安溪县公安局	384.99	38.50	-	受政府财政预算影响,付款审批进度推迟	-
4	石化盈科信息技术有限责任公司	311.00	15.55	311.00	客户隶属大型集团,付款流程复杂	100%
5	乌鲁木齐市公安局	280.83	23.61	9.93	受政府财政预算影响,付款审批进度推迟	3.54%
6	广东省政务服务数据管理局	263.76	13.19	263.76	受政府财政预算影响,付款审批进度推	100%

					迟	
7	贺州市公安局	250.00	25.00	-	受政府财政预算影响,付款审批进度推迟	-
8	武夷山市公安局	212.08	63.62	92.75	受政府财政预算影响,付款审批进度推迟	43.73%
9	北京神州泰岳教育科技有限公司	209.00	20.90	-	款项于 2020 年预计无法收回,已于 2020 年全额计提坏账准备	-
10	河南信大网御科技有限公司	196.00	9.80	196.00	客户付款流程较为复杂,付款周期较长	100%
11	湖南雨人网络安全技术股份有限公司	180.00	18.00	40.00	最终用户款项尚未收回完毕	22.22%
12	浙江省公安厅	168.00	8.40	168.00	受政府财政预算影响,付款审批进度推迟	100%
13	中国人民解放军	149.24	7.46	149.24	受单位安排影响,付款审批进度推迟	100%
14	华威益腾(北京)科技有限公司	140.00	70.00	140.00	该客户未收到最终用户款项,故未相应支付给公司	100%
15	广西戴亚柯仑信息科技有限公司	137.70	6.89	-	该客户未收到最终用户款项,故未相应支付给公司	-
16	南京烽火星空通信发展有限公司	135.10	13.51	135.10	最终用户款项尚未收回完毕	100%
17	四川省畅达运输有限责任公司	132.00	13.20	132.00	受政府财政预算影响,付款审批流程较长	100%
18	武汉白虹软件科技有限公司	104.31	10.43	6.00	款项于 2021 年上半年预计无法收回,已于 2021 年上半年单项计提坏账准备	5.75%
19	丽水市公安局	104.00	11.40	79.20	受政府财政预算影响,付款审批流程较长	76.15%
20	北京市公安局	101.28	10.13	101.28	受政府财政预算影响,付款审批流程较长	100%
合计		4,938.39	533.14	3,303.36	-	66.89%

4、2018 年 12 月 31 日逾期应收账款

单位：万元

序号	客户名称	逾期金额	逾期部分坏账准备金额	逾期部分分期后回款金额	逾期原因	逾期部分截至 2021 年 11 月 30 日回款比例
1	南京市公安局	1,155.00	57.75	1,155.00	受政府财政预算影响，付款审批流程较长	100%
2	南京烽火星空通信发展有限公司	504.72	45.10	504.72	该客户尚未将最终用户款项收回完毕，故未相应支付给公司	100%
3	安溪县公安局	384.99	19.25	-	受政府财政预算影响，付款审批流程较长	-
4	成都天府新区投资集团有限公司	350.00	17.50	350.00	付款审批流程延后	100%
5	江西省公安厅	267.60	13.38	267.60	受政府财政预算影响，付款审批流程较长	100%
6	贺州市公安局	250.00	12.50	-	受政府财政预算影响，付款审批流程较长	-
7	二三八单位	239.20	23.92	239.20	受财政预算影响，付款审批流程较长	100%
8	湖南雨人网络安全技术股份有限公司	210.00	10.50	160.00	该客户尚未将最终用户款项收回完毕，故未相应支付给公司	76.19%
9	北京神州泰岳教育科技有限公司	209.00	10.45	-	款项于 2020 年预计无法收回，已于 2020 年全额计提坏账准备	-
10	武夷山市公安局	206.73	20.67	206.73	受政府财政预算影响，付款审批流程较长	100%
11	乌鲁木齐市公安局	181.35	9.07	-	受政府财政预算影响，付款审批流程较长	-
12	福州市公安局	170.00	17.00	170.00	受政府财政预算影响，付款审批流程较长	100%
13	北京华威益腾通讯技术有限公司	164.40	16.44	164.40	该客户未收到最终用户款项，故未相应支付给公司	100%
14	华威益腾（北京）科技有限公司	140.00	42.00	140.00	该客户未收到最终用户款项，故未相应支付给公司	100%
15	四川省畅达运输有限责任公司	132.00	6.60	132.00	该客户未收到最终用户款项，故未相应支付给公司	100%
16	安徽新华博信息技术股份有限公司	129.60	18.36	129.60	该客户未收到最终用户款项，故未相应支付给公司	100%

17	八二三单位	115.50	34.65	115.50	受单位安排影响，付款 审批进度推迟	100%
合计		4,810.09	375.14	3,734.75	-	77.64%

报告期内，公司逾期应收账款客户主要包括政府单位、军队和集成商等。其中，政府单位和军队由于受政府财政预算和单位统一安排等因素影响，付款审批流程较长，存在逾期情形。公司集成商客户应收账款逾期原因主要由于终端用户付款延迟，集成商客户对应的终端用户主要为政府单位，由于回款资金受政府预算影响，导致报告期内回款逾期。

虽然公司应收账款存在一定逾期现象，但回款周期较为稳定，坏账计提较为充分。截至 2021 年 11 月 30 日，公司持续收回逾期款项，报告期各期末逾期应收账款的期后回款比例如下：

单位：万元

期间	逾期应收账款账面余额	逾期应收账款期后回款金额	期后回款比例
2021 年 6 月 30 日	6,887.68	2,887.17	41.92%
2020 年 12 月 31 日	5,614.11	2,671.81	47.59%
2019 年 12 月 31 日	6,971.54	5,031.19	72.17%
2018 年 12 月 31 日	6,964.11	5,385.52	77.33%

如上表所示，公司报告期各期末的逾期应收账款仍在持续收回。2020 年末及 2021 年 6 月末的逾期应收账款回款比例较低，主要系期后回款与逾期应收账款形成时点的间隔相比以前年度较短而形成。

（二）2020 年末长账龄应收账款占比较高的原因

2020 年公司账龄为 2-3 年、3-4 年的应收账款占比大幅上升，主要原因在于，公司 2020 年新增业务回款情况较好，年末应收账款账面余额较上年末有所下降，因此 2017 年至 2018 年部分业务产生的尚未收回的应收账款累积占比上升。此外，受 2020 年疫情影响，2017 年至 2018 年部分业务产生的尚未收回的应收账款回款速度有所降低。

2020 年末，账龄 3-4 年的应收账款对应的主要客户及未收回完毕的原因如下：

单位：万元

客户名称	应收账款 账面 余额	坏账准 备金额	2019 年 末余额	2020 全 年回款 率	2020 年末收回完毕原因
北京华威益腾通讯技术有限公司	164.40	82.20	164.40	-	该客户未收到最终用户款项，故未相应支付给公司

武夷山市公安局	119.33	59.66	229.30	47.96%	受政府财政预算影响，付款审批推迟
北京华信安天信息科技有限公司	45.00	22.50	45.00	-	该客户未收到最终用户款项，故未相应支付给公司
福州市公安局	34.00	17.00	34.00	-	受政府财政预算影响，付款审批推迟
天津市楚海文化传播有限公司	30.00	30.00	30.00	-	已确认为坏账并全额计提坏账准备

2020 年末，账龄 2-3 年的应收账款对应的主要客户及未收回完毕的原因如下：

单位：万元

客户名称	应收账款金额	坏账准备金额	2019 年末余额	2020 全年回款率	2020 年末未收回完毕原因
安溪县公安局	384.99	115.50	449.15	14.29%	受政府财政预算影响，付款审批推迟
贺州市公安局	250.00	75.00	350.00	28.57%	受政府财政预算影响，付款审批推迟
南京市公安局	218.74	65.62	770.00	71.59%	受政府财政预算影响，付款审批推迟
北京神州泰岳教育科技有限公司	209.00	209.00	209.00	-	已确认为坏账并全额计提坏账准备
乌鲁木齐市公安局	195.30	58.59	195.30	-	受新疆疫情影响，付款审批进度推迟
湖南雨人网络安全技术股份有限公司	140.00	42.00	180.00	22.22%	最终用户款项尚未收回完毕
南京烽火星空通信发展有限公司	135.10	40.53	135.10	-	该客户未收到最终用户款项，故未相应支付给公司
武汉白虹软件科技有限公司	98.31	29.49	104.31	5.75%	2021 年上半年，相关款项预计无法收回，已单项计提坏账准备
河南众诚信息科技股份有限公司	84.00	25.20	84.00	-	该客户未收到最终用户款项，故未相应支付给公司
丽水市公安局	59.40	17.82	138.60	57.14%	受政府财政预算影响，付款审批推迟
杭州禹森科技有限公司	38.00	11.40	38.00	-	受疫情影响，付款进度推迟
广州市公安局天河分局	30.47	9.14	60.95	50.00%	受政府财政预算影响，付款审批推迟

2020 年末，公司长账龄应收账款主要由于政府单位受财政预算影响推迟付款流程而形成，该类客户具备良好的信誉及偿付能力，且与公司合作稳定。公司已按照账龄分析法对不同期限的应收账款进行了坏账准备的计提，并对部分预计无法收回的应收账款进行了单项计提坏账准备，坏账准备计提充分。

（三）2021 年 6 月末长账龄应收账款占比较高的原因

2021年6月末应收账款账面余额中,账龄2-3年及3-4年的应收账款账面余额占比28.02%,占比较高,主要原因包括:

1、2021年6月末与2020年末间隔时间较短,由于发行人客户付款审批等进度较慢,且部分地市仍受疫情影响,致使2020年末账龄较长的应收账款的回款情况在2021年6月末无明显改善;

2、由于部分客户资金状况异常,导致相关款项在2021年1-6月无法收回,公司已对该等款项单项计提坏账准备。2021年6月末,账龄2-3年应收账款账面余额中,已单项计提坏账准备金额占比25.56%;账龄3-4年应收账款账面余额中,已单项计提坏账准备金额占比8.04%。

2021年6月末,账龄3-4年的应收账款对应的主要客户及未收回完毕的原因如下:

单位:万元

客户名称	应收账款账面余额	坏账准备金额	2020年末余额	2021年1-6月回款率	2021年6月末未收回完毕原因
安溪县公安局	449.15	224.58	384.99	-	受政府财政预算影响,付款审批推迟
贺州市公安局	350.00	175.00	250.00	-	受政府财政预算影响,付款审批推迟
北京华威益腾通讯技术有限公司	164.40	82.20	164.40	-	该客户未收到最终用户款项,故未相应支付给公司
武夷山市公安局	119.33	59.66	119.33	-	受政府财政预算影响,付款审批推迟
南京烽火星空通信发展有限公司	57.90	28.95	135.10	57.14%	该客户未收到最终用户款项,故未相应支付给公司
北京华信安天信息科技有限公司	45.00	22.50	45.00	-	该客户未收到最终用户款项,故未相应支付给公司
北京启明星辰信息安全技术有限公司	39.44	19.72	23.85	-	该客户未收到最终用户款项,故未相应支付给公司
天津市楚海文化传播有限公司	30.00	30.00	30.00		已确认为坏账并全额计提坏账准备

注:安溪县公安局、贺州市公安局2021年6月末应收账款账面余额大于2020年末应收账款账面余额的原因系质保金于2021年上半年到期。

2021年6月末,账龄2-3年的应收账款对应的主要客户及未收回完毕的原因如下:

单位:万元

客户名称	应收账	坏账准	2020年	2021年	2021年6月末未收回完毕原因
------	-----	-----	-------	-------	-----------------

	款账面 余额	备金额	未余额	1-6 月回 款率	
南京市公安局	218.74	65.62	218.74	-	受政府财政预算影响，付款审批推迟
北京神州泰岳教育科技有限公司	209.00	209.00	209.00	-	已确认为坏账并全额计提坏账准备
乌鲁木齐市公安局	195.30	58.59	195.30	-	受新疆疫情影响，付款审批进度推迟
湖南雨人网络安全技术股份有限公司	140.00	42.00	140.00	-	最终用户款项尚未收回完毕
武汉白虹软件科技有限公司	82.64	82.64	82.64	-	已确认为坏账并全额计提坏账准备
河南众诚信息科技股份有限公司	84.00	25.20	84.00	-	该客户未收到最终用户款项，故未相应支付给公司
丽水市公安局	59.40	17.82	59.40	-	受政府财政预算影响，付款审批推迟
湖北儒晓科技有限公司	56.00	16.80	56.00	-	该客户未收到最终用户款项，故未相应支付给公司
杭州禹森科技有限公司	35.00	10.50	38.00	7.89%	受疫情影响，付款进度推迟
广州市公安局天河区分局	30.47	9.14	30.47	-	受政府财政预算影响，付款审批推迟

（四）最终用户款项未收回完毕致使应收账款逾期或账龄较长的客户情况

1、应收账款主要逾期债务人

上文“（一）逾期应收账款”所披露的发行人应收账款主要逾期债务人中，除已单项计提坏账准备的债务人外，由于最终用户款项未收回完毕而截至 2021 年 11 月 30 日未完成回款的主要应收账款逾期债务人情况如下：

客户名称	终端用户类别	是否属于集成商
厦门安胜网络科技有限公司	公安单位	是
广西戴亚柯仑信息科技有限责任公司	公安单位	是
上海安询信息技术有限公司	公安单位	是
湖南雨人网络安全技术股份有限公司	公安单位	是

如上表所示，由于终端用户款项未收回完毕致使相关款项截至 2021 年 11 月 30 日仍未收回完毕的逾期债务人均均为集成商客户，相关终端用户为公安单位。

2、应收账款主要长账龄债务人

上文“（二）2020 年末长账龄应收账款占比较高的原因”及“（三）2021 年 6 月末长账龄应收账款占比较高的原因”所披露的发行人应收账款主要长账龄债务人中，除已单项计提坏账准备的债务人外，由于最终用户款项未收回完毕而

导致 2021 年 6 月末应收账款账龄在 2 年以上的主要债务人情况如下：

单位：万元

客户名称	2021 年 6 月 30 日 应收账款账面余 额	终端用户类别	是否属于集 成商	截至 2021 年 11 月 30 日回款比例
北京华信安天信 息科技有限公司	45.00	政府单位	是	100%
湖南雨人网络安 全技术股份有限 公司	140.00	公安单位	是	-
河南众诚信息科 技股份有限公司	84.00	公安单位	是	-
湖北儒晓科技有 限公司	56.00	高校	是	-
北京启明星辰信 息安全技术有限 公司	39.44	国有企业、高校 及公安单位	是	5.70%
南京烽火星空通 信发展有限公司	57.90	公安单位	是	100%
北京华威益腾通 讯技术有限公司	164.40	政府单位	是	100%

如上表所示，上述长账龄应收账款主要债务人均为集成商客户，终端用户主要为政府单位、公安单位和高校等。

3、相关收入确认方式

客户名称	合同金额	2021 年 6 月 30 日应收账 款账面余额	相关收入确认时间	相关收入确认依据
厦门安胜网络 科技有限公司	430.00	258.00	2021 年 1-6 月	集成商出具的终验报告
广西戴亚柯仑 信息科技有限 责任公司	162.00	162.00	2019 年	集成商出具的终验报告
上海安询信息 技术有限公司	222.00	155.40	2019 年	集成商出具的终验报告
湖南雨人网络 安全技术股份 有限公司	180.00	140.00	2018 年	集成商出具的终验报告
河南众诚信息 科技股份有限 公司	120.00	84.00	2018 年	集成商出具的终验报告
北京华信安天 信息科技有限	45.00	45.00	2017 年	集成商出具的终验报告

公司				
湖北儒晓科技有限公司	86.00	56.00	2019 年	集成商出具的终验报告
北京启明星辰信息安全技术有限公司	112.80	39.44	2018 年	集成商出具的终验报告
北京华威益腾通讯技术有限公司	822.00	164.40	2017 年	集成商出具的终验报告

如上表所示，相关收入确认的依据为集成商客户出具的终验报告。在非直销且客户收到最终用户款项后付款的模式下，公司收入确认政策与已在科创板上市的同行业可比公司或业务模式相近的软件和信息技术服务业公司保持一致，具体情况如下：

公司名称	收入确认方式
安博通	产品交付后并获取非最终用户收货验收单或对账单/系统对账单确认收入
品高软件	按直接客户验收确认收入，客户收到最终用户款项后付款仅影响公司收款时间，不形成项目验收条件的一部分
中科通达	按直接客户验收确认收入，客户收到最终用户款项后付款对收入确认政策不构成影响
发行人	按直接客户（即集成商）出具的验收报告确认收入

如上表所示，同行业可比公司或业务模式相近的软件和信息技术服务业公司在非直销模式下，以直接客户出具的验收报告作为收入确认依据，客户收到最终用户款项后付款仅为结算政策，对收入确认方式不构成影响。综上所述，发行人相关收入政策符合行业惯例，具有合理性。

（五）发行人应收账款坏账准备计提比例与同行业可比上市公司的对比

在应收款项坏账准备计提比例方面，公司与同行业可比上市公司不存在重大差异，具体如下：

可比上市公司	1 年以内	1-2 年	2-3 年	3-4 年	4-5 年	5 年以上
启明星辰	0.5%	8.00%	20.00%	50.00%	50.00%	100%
美亚柏科	5.00%	10.00%	30.00%	50.00%	80.00%	100%
绿盟科技	7.17%	23.31%	47.66%	67.06%	83.84%	100%
深信服	0-6 个月：2.50% 7-12 个月：15.00%	35.00%	70.00%	100%	100%	100%
安恒信息	5.00%	10.00%	30.00%	100%	100%	100%
安博通	0-6 个月：1.00%	30.00%	50.00%	100%	100%	100%

可比上市公司	1 年以内	1-2 年	2-3 年	3-4 年	4-5 年	5 年以上
	7-12 个月：10.00%					
山石网科	2.15%	9.56%	23.52%	48.02%	80.75%	100%
奇安信	5.00%	15.00%	30.00%	50.00%	80.00%	100%
行业均值	4.88%	17.61%	37.65%	70.63%	84.32%	100%
永信至诚	5.00%	10.00%	30.00%	50.00%	80.00%	100%

公司已制定了合理、谨慎的应收账款坏账准备计提政策，报告期内按照上述政策充分计提了坏账准备。

公司应收账款坏账准备计提比例低于深信服、安恒信息、奇安信及山石网科的主要原因系深信服、安恒信息、奇安信及山石网科销售模式更加侧重于渠道销售，由于客户群体中经销商较多，坏账计提也更为谨慎。而发行人销售模式以直销为主，客户集中于政府单位、军队、国有企业和高校，客户信用情况较佳。

如剔除业务模式与发行人差异相对较大的深信服、安恒信息、奇安信及山石网科，则公司与其他同行业可比上市公司的坏账准备计提情况比较如下：

可比上市公司	1 年以内	1-2 年	2-3 年	3-4 年	4-5 年	5 年以上
启明星辰	0.5%	8.00%	20.00%	50.00%	50.00%	100%
美亚柏科	5.00%	10.00%	30.00%	50.00%	80.00%	100%
绿盟科技	7.17%	23.31%	47.66%	67.06%	83.84%	100%
安博通	0-6 个月：1.00% 7-12 个月：10.00%	30.00%	50.00%	100%	100%	100%
行业均值	4.54%	17.83%	36.92%	66.77%	78.46%	100%
永信至诚	5.00%	10.00%	30.00%	50.00%	80.00%	100%

如发行人将账龄 1 年以上的应收账款按照上表中的行业坏账准备计提比例均值计提坏账准备，则该情况对报告期各期净利润的影响如下：

单位：万元

项目	2021 年 1-6 月	2020 年	2019 年	2018 年
净利润	-2,033.94	4,229.58	162.63	331.91
按同行业平均坏账准备计提比例模拟测算后的净利润	-2,393.79	3,935.83	-189.29	110.80

如上表所示，按照同行业平均坏账准备计提比例计提坏账准备对发行人净利润产生一定影响。但发行人选择的上市标准为“预计市值不低于人民币 10 亿元，最近一年净利润为正且营业收入不低于人民币 1 亿元”，故该等情形对发行人符

合上市标准不构成实质性影响。

请保荐机构、申报会计师对上述事项进行核查，说明对报告期各期末应收账款的核查情况。

【核查程序】

保荐机构及申报会计师执行了以下核查程序：

（一）函证

保荐机构及申报会计师对报告期内主要客户及主要债务人执行函证程序，发函及回函的具体比例如下：

单位：万元

项目	2021.6.30	2020.12.31	2019.12.31	2018.12.31
应收账款账面余额	9,101.08	9,997.65	10,978.56	10,451.18
发函金额	7,906.31	8,765.87	10,115.44	10,349.89
函证程序可确认金额	7,906.31	8,765.87	10,115.44	10,349.89
其中：回函相符金额	6,349.68	7,181.79	7,619.44	8,438.05
回函不符并执行替代测试金额	-	-	166.60	-
未回函并执行替代测试金额	1,556.63	1,584.08	2,329.41	1,911.84
发函金额占应收账款账面余额比例	86.87%	87.68%	92.14%	99.03%
回函相符金额占发函金额比例	80.31%	81.93%	75.32%	81.53%
回函相符金额占应收账款账面余额比例	69.77%	71.83%	69.40%	80.74%
函证程序可确认金额占发函金额比例	100%	100%	100%	100%
函证程序可确认金额占应收账款账面余额比例	86.87%	87.68%	92.14%	99.03%

报告期内，应收账款函证回函相符金额占发函金额比例均在 75%以上。针对回函不符及未回函的应收账款函证，保荐机构及申报会计师通过获取相关合同、验收单、记账凭证、发票及期后回款凭证执行替代测试。经替代测试核查，回函不符及未回函的应收账款金额真实、准确。

（二）走访

保荐机构及申报会计师对报告期内主要客户及主要债务人执行走访程序，了解其与发行人的业务合作情况，走访金额及比例的具体情况如下表所示：

单位：万元

项目	2021.6.30	2020.12.31	2019.12.31	2018.12.31
期末应收账款余额	9,101.08	9,997.65	10,978.56	10,451.18
走访客户应收账款余额	4,875.89	6,337.34	5,670.10	5,211.21
应收账款走访覆盖率	53.57%	63.39%	51.65%	49.86%

（三）其他程序

1、访谈发行人财务总监，了解报告期内公司客户的主要构成、合作情况、销售回款和逾期情况；

2、获取公司报告期各期末的应收账款账龄明细表，了解账期超过 1 年的应收账款的原因，分析原因的合理性；访谈发行人财务总监，了解 2020 年账龄为 2-3 年、3-4 年的应收账款占比较高的原因，结合 2020 年应收账款明细表对其原因进行分析；

3、获取发行人报告期各期末的应收账款逾期明细表，了解逾期客户的经营情况、项目情况和逾期原因，分析逾期原因的合理性以及款项未来的可回收性；

4、获取发行人报告期各期末的应收账款期后回款明细表，通过查看银行回单等回款原始凭证，核查期后回款金额的真实性、准确性；访谈发行人财务总监，了解期后回款比例较低的原因，结合对部分客户走访了解的回款安排等事项，分析期后回款比例较低的原因的合理性；

5、通过网络检索公司应收账款主要债务人信息，核查是否存在经营异常的主要债务人。

【核查意见】

经核查，保荐机构和申报会计师认为：发行人期后回款比例较低主要系受政府财政预算、客户审批流程较慢等因素影响所致，导致部分款项出现了逾期；发行人 2020 年账龄为 2-3 年、3-4 年的应收账款占比金额大幅上升，主要系政府机关客户受政府财政预算限制付款进度延期等因素所致。

11、关于存货

根据申报材料：（1）报告期各期末存货的账面价值分别为 1,475.00 万元、2,401.62 万元和 2,703.34 万元，包括原材料、库存商品及项目成本，其中（合同履约成本）分别为 1,237.05 万元、1,961.87 万元和 2,346.48 万元；（2）项目成本包括直接材料、直接人工、外购软件及服务和其他费用，2019 年、2020

年跌价准备金额分别为 16.13 万元和 249.88 万元，系公司已提前开工尚未签订合同的项目。

请发行人说明：（1）报告期各期末项目成本的库龄情况，库龄较长的项目成本及原因，相关合同的签订时间及后续验收情况，存货跌价准备计提的充分性；

（2）公司已提前开工尚未签订合同的项目成本计入存货并计提跌价准备是否符合企业会计准则的规定，后续签订合同后的会计处理。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见，说明对发行人项目成本的核查情况。

【回复】

（1）报告期各期末项目成本的库龄情况，库龄较长的项目成本及原因，相关合同的签订时间及后续验收情况，存货跌价准备计提的充分性；

一、报告期各期末项目成本的库龄情况

报告期各期末，公司项目成本的库龄情况如下：

单位：万元

类别	库龄	2021.6.30		2020.12.31		2019.12.31		2018.12.31	
		金额	占比	金额	占比	金额	占比	金额	占比
合 同 履 约 成 本/ 项 目 成 本 账 面 余 额	1 年以 内	2,542.88	62.56%	1,997.03	76.92%	1,684.97	85.19%	1,182.20	95.57%
	1-2 年	928.33	22.84%	378.93	14.59%	238.18	12.04%	54.85	4.43%
	2-3 年	373.07	9.18%	181.95	7.01%	54.85	2.77%	-	-
	3 年以 上	220.39	5.42%	38.44	1.48%	-	-	-	-
	小计	4,064.68	100%	2,596.36	100%	1,978.00	100%	1,237.05	100%

报告期内，公司承接的网络安全项目数量增多、项目规模增大，导致 2018 年末至 2021 年 6 月末的合同履约成本/项目成本金额逐年增加。2020 年末及 2021 年 6 月末，公司在建周期超过 1 年的合同履约成本/项目成本金额及占比增长较大，主要原因系受新冠疫情影响，部分项目周期拉长，截至 2020 年末及 2021 年 6 月末尚未完成验收。

二、库龄较长的项目成本及原因，相关合同的签订时间及后续验收情况

报告期内，公司合同履约成本/项目成本库龄一年以上的的主要项目具体情况，相关合同的签订时间及后续验收情况如下：

（一）2021 年 1-6 月合同履约成本库龄一年以上的的主要项目：

单位：万元

客户单位	项目	合同履行成本(账面余额)	库龄一年以上的金额(账面余额)	合同签订时间	长时间未验收的原因	验收情况
广东省公安厅	广东省公安网络靶场	708.91	267.18	2020年11月26日	受政府部门内部程序影响，导致合同签署、试运行和验收有所延后。2021年5月，该项目完成部署，但试运行周期较长，使得项目于2021年12月进行终验。	2021年12月3日验收
南京市公安局	网络安全实验室二期	233.90	233.75	2021年7月10日	该项目系公司2018年收入确认项目南京网络安全实验室项目的延伸项目。2020年，受疫情影响，南京市公安局相关预算无法进一步落实，致使项目处于停滞状态，合同签订及后续验收安排延后。2021年7月，随着相关预算落实并签订合同，公司逐步恢复项目实施，预计于2021年12月末完成终验。	已完成项目实施，正处于验收阶段
常州市公安局	网络安全实验室项目	191.63	188.90	2019年12月30日	该项目已于2020年6月进入试运行阶段，但由于客户单位统一安排及新冠疫情等原因影响，终验时间推迟至2021年8月。	2021年8月31日验收
浙江大学	网络安全课题项目	107.54	95.76	2019年9月3日	在该项目中，公司负责的课题为浙江大学网络安全相关课题的一部分。由于该项目专业指标要求较高，且浙江大学拟对所有网络安全相关课题集中验收，使得项目实施周期较长，验收时间延后。	已完成项目实施，正处于验收阶段
广东省政务服务	信息化服务项目	231.86	94.51	2020年9月1日	受新冠疫情影响，项目集中部署时间有所延后，实施周期较长。	已完成项目实施，正处于验收

务数 据管 理局						阶段
----------------	--	--	--	--	--	----

(二) 2020 年度合同履约成本库龄一年以上的重大项目:

单位: 万元

客户单位	项目	合同履约成本(账面余额)	库龄一年以上的金额(账面余额)	合同签订时间	长时间未验收的原因	验收情况
广东省公安厅	广东省公安网络靶场	267.18	264.76	2020 年 11 月 26 日	同上	同上
南京市公安局	网络安全实验室二期	233.75	205.85	2021 年 7 月 10 日	同上	同上
浙江大学	网络安全课题项目	95.76	66.25	2019 年 9 月 3 日	同上	同上
中国科学院信息工程研究所	网络安全环境建设项目	72.47	39.16	2020 年 4 月 3 日	该项目服务于科研院所, 实施周期和试运行周期较长, 验收时间相对延后。2021 年 1 月, 该项目完成部署工作, 试运行周期于 2021 年 2 月持续至 2021 年 7 月。	2021 年 8 月 31 日验收

注: 公司基于客户业务情况, 部署南京市公安局“网络安全实验室二期项目”。但 2020 年受新冠疫情影响, 该项目处于停滞状态, 公司基于谨慎性判断该项目的预计可变现净值为零, 已于 2020 年底将该项目的履约成本全额计提跌价准备。随着 2021 年新冠疫情影响逐渐降低, 公司于 2021 年 7 月 10 日与南京市公安局正式签订“网络安全实验室二期项目”合同, 并恢复项目实施。

(三) 2019 年度合同履约成本库龄一年以上的重大项目:

单位: 万元

客户单位	项目	合同履约成本(账面余额)	库龄一年以上的金额(账面余额)	合同签订时间	长时间未验收的原因	验收情况
广东省公安厅	广东省公安网络靶场	281.17	208.07	2020 年 11 月 26 日	同上	同上
南京市公安局	网络安全实验室二期	205.85	28.71	2021 年 7 月 10 日	同上	同上

(四) 2018 年度合同履约成本库龄一年以上的重大项目:

单位: 万元

客户单位	项目	合同履约成本(账面余额)	库龄一年以上的金额(账面余额)	合同签订时间	长时间未验收的原因	验收情况
广东省公安厅	广东省公安网络靶场	208.07	54.83	2020 年 11 月 26 日	同上	同上

报告期内, 广东省公安厅项目及南京市公安局项目的项目成本库龄较长, 具体原因如下:

广东省公安厅靶场平台项目系公司 2018 年 6 月已确认收入项目的延伸项目, 该项目的合同金额较大, 项目实施内容复杂程度较高。公司基于与客户的长期合作关系, 考虑客户的业务情况, 响应客户需求提前部署。在项目实施期间内, 公司严格按照前期的项目规划、预算及客户的实际要求进行项目建设, 并保持与客户持续的沟通, 确认该项目具备实施必要性并符合客户要求。但受政府部门内部程序影响, 合同签订时间较为延后。公司已于 2020 年 11 月与客户完成了合同的签订工作。

南京市公安局网络安全实验室二期项目系公司 2018 年收入确认项目南京网络安全实验室项目的延伸项目。公司基于客户业务情况, 在未签订合同前, 已部署该项目。2020 年, 受疫情影响, 南京市公安局相关预算无法进一步落实, 因公司暂时无法与南京市公安局针对该项目签订业务合同或者其他替代性协议, 该项目已处于停滞状态, 公司基于谨慎性判断该项目的预计可变现净值为零, 已于 2020 年底将该项目的履约成本全额计提跌价准备。

三、报告期各期末项目成本中未签订合同即开工项目占比

报告期各期末, 公司基于客户业务需求, 存在签订合同前即配合客户部署项目的情况, 报告期内各期末项目成本的账面余额中, 该类情形的具体金额及比例如下:

单位: 万元

时间	项目成本期末账面余额中发生于合同签订时间前的金额	项目成本期末账面余额中发生于合同签订时间前的金额(当期新增)	项目成本期末账面余额中发生于合同签订时间前的金额占比
----	--------------------------	--------------------------------	----------------------------

2021 年 1-6 月/2021.6.30	758.69	149.66	18.67%
2020 年/2020.12.31	661.91	139.30	25.19%
2019 年/2019.12.31	729.53	492.75	36.88%
2018 年/2018.12.31	270.03	215.20	21.83%

报告期各期末，项目成本中存在合同签订前即开展项目部署的情况，主要系相关项目的非标准化程度和复杂程度普遍较高，公司响应客户实际需求，提前以现场沟通、开展技术试点等方式参与项目部署。报告期各期末，因提前开展项目部署而形成的项目成本金额占报告期各期末项目成本账面余额的比例相对较低。

四、存货跌价准备计提的充分性

（一）存货跌价准备计提的依据和方法

公司按照项目口径核算项目成本，将各项目成本对应到具体项目合同。公司的项目成本主要包括硬件及部分软件的外部采购、分包支出、人工支出及其他费用。根据企业会计准则的相关要求，持有目的为项目建设采购的存货，在正常建设过程中以所生产的产成品的估计未来现金流入减去至完工时估计将要发生的成本、估计的费用和相关税费后的金额确定其可变现净值。

公司网络安全业务项目实施周期一般在一年以内。资产负债表日，公司考虑在施项目的客户情况、合同资料（预计签订合同情况）、项目施工周期、项目预算的执行等因素，以项目对应的合同价格（预计合同价格）、已发生的项目成本及项目预算为基础确认项目的可变现净值，具体方法为将项目合同价格（预计合同价格）确认为产成品的估计售价，根据项目的实际施工情况及预算的执行情况确认项目完工时估计还要发生的项目成本，剔除相关税费的影响后确认单个项目的可变现净值。

（二）存货跌价计提的充分性

在各资产负债表日，由于项目中止实施，暂时未签订合同，预计可变现净值为零而全额计提跌价的项目成本余额分别为 0 万元、16.13 万元、249.88 万元和 249.88 万元，占项目成本账面余额比例分别为 0%、0.82%、9.62%和 6.15%。除此之外，其他项目均在正常执行中，公司按照上述既定的存货跌价准备计提政策，充分考虑影响项目可变现净值的各项因素，对存货的每个项目均执行减值测试程序。经对各项目单独进行减值测试，公司已签订合同的各个项目存货可变现净值均高于项目成本，因此无需计提存货跌价准备。

(2) 公司已提前开工尚未签订合同的项目成本计入存货并计提跌价准备是否符合企业会计准则的规定，后续签订合同后的会计处理。

一、公司已提前开工尚未签订合同的项目成本计入存货是否符合企业会计准则的规定

根据《企业会计准则第1号——存货》第三条规定，“存货是指企业在日常活动中持有以备出售的产成品或商品、处在生产过程中的在产品、在生产过程或提供劳务过程中耗用的材料和物料等”以及第四条“存货同时满足下列条件的，才能予以确认，（1）与该存货有关的经济利益很可能流入企业，（2）该存货的成本能够可靠地计量。”公司在基本确定能获取合同的情况下，才会将开发成本作为项目成本计入存货。如南京市公安局网络安全实验室二期项目，该项目的一期即由公司承担建设。二期项目是一期项目的延续和深度开发，经过与南京市公安局确认后，公司提前采购并进行研究开发。由于该项目短期内受新冠疫情影响，可能无法签订业务合同或者其他类似协议，但考虑该项目系一期项目的延续和深度开发，同时结合前期建设期间与客户的沟通及客户的实际需求，公司认为该项目待新冠疫情结束或者减缓后，客户会尽快推动签订合同及项目建设。公司认为该存货有关的经济利益很可能流入企业并计入存货。

综上所述，公司是在基本确定能获取合同的情况下，将开发成本作为项目成本计入存货，符合企业会计准则的相关规定。

二、公司将尚未签订合同的计提跌价准备是否符合企业会计准则的规定

公司项目具有定制化、复杂程度高等特点，项目周期一般在3个月到一年以内，对于在建周期较长以上且未尚未签订合同的项目，报告期内末公司会根据签订合同进度（如招投标进度、预计签订进度）进行评估，基于谨慎性考虑，将项目状态异常且仍无法确定是否签订合同的对应项目的可变现净值确认为零。根据《企业会计准则第1号——存货》第十六条“企业确定存货的可变现净值，应当以取得的确凿证据为基础，并且考虑持有存货的目的、资产负债表日后事项的影响等因素。”以及第十七条“为执行销售合同或者劳务合同而持有的存货，其可变现净值应当以合同价格为基础计算”，公司存货在进行减值测试时，应将单个项目的项目成本作为一个整体，以项目合同价格为可变现净值计算的基础。

综上所述，公司将项目状态异常且预计无法签订合同的项目的计提跌价准备

符合企业会计准则的规定。

三、后续签订合同后的会计处理

公司制定了《项目管理制度》，销售部门项目负责人根据未签订项目实际执行情况持续与客户进行沟通。每个月由项目经理将沟通结果通报销售部门经理，销售部门经理根据实际情况判断短期内签订合同的可能性，并将信息通报公司产销统计中心，并按月编制《项目执行情况表》，每季度销售部门经理将提前开工尚未签订的项目根据与客户沟通的结果，判断预计合同签订时间，将短时间内无法预计或无法签订合同的项目通报财务部，销售部门根据已经发生的成本金额，提交总经理审议，总经理审议通过后，财务部将短时间无法签订合同的项目计提存货跌价。

项目经理继续持续跟踪项目成果判断后续签订合同的可能性，合同签订后，项目经理通告财务人员并重新计算存货跌价，并将已计提的存货跌价准备进行转回的会计处理。如持续跟踪一段时间后，客户明确已计提跌价的项目未来合同无法签订，项目经理将消息通告部门经理，并提交总经理审议，总经理审议通过后，财务部进行存货核销的会计处理。

四、公司确认合同签订可行性的具体方法

公司的项目负责人及销售人员持续与客户沟通并跟踪合同状态。公司制定了《项目执行情况表》，由销售部门经理按具体项目情况填写。根据客户的实际反馈情况及《项目执行情况表》的填报结果，公司按月度持续、及时地关注合同签订进展，确保了合同签订的可行性。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见，说明对发行人项目成本的核查情况。

【回复】

保荐机构及申报会计师对报告期各期末发行人项目成本进行了审慎核查，核查方法、核查程序及核查结论具体如下：

1、实地走访 2020 年末项目成本涉及的主要客户单位，了解相关项目的实施进度及预计验收时间。经核查，实地走访涉及的相关项目的验收时间或预计验收时间均在资产负债表日后。

2、实地走访报告期各期末项目成本账面余额涉及的主要客户单位，了解相

关项目截至资产负债表日的实施进度，了解部分项目先于合同签订时间开工的背景。经核查，相关项目均为截至资产负债表日正在实施的项目，发行人先于合同签订时间部署项目实施主要基于客户对技术指标的复杂要求。

3、访谈发行人总经理及财务总监，获取发行人销售人员编制的《项目执行情况表》，核查发行人是否制定了跟踪合同签订的有效措施。经核查，发行人销售人员有效跟踪合同签订进度，发行人已制定跟踪合同签订的内控措施。

4、获取报告期各期末项目成本对应的主要销售合同，核查合同签订时点、合同约定的实施周期是否与报告期各期末项目成本余额相匹配。经核查，发行人报告期各期末项目成本对应的主要项目为正在执行且尚未确认收入的项目，项目背景、合同签订时间与项目成本核算具备匹配关系。

5、访谈发行人财务负责人，了解发行人存货跌价准备计提政策，并测算报告期各期末项目成本对应的主要项目的可变现净值，核查存货跌价准备计提是否充分、合理。经核查，发行人有效执行了存货跌价准备计提政策，存货跌价准备计提具有合理性。

6、获取发行人项目工时拆分表，核查报告期各期末项目成本对应的主要项目的实施人员构成；并将项目工时拆分表中的人员薪酬与项目成本明细表中的人员薪酬进行比对。经核查，报告期各期末项目成本对应的主要项目由发行人员工有效参与实施，项目成本中的人员薪酬与项目工时拆分表记录一致。

7、获取项目成本中的硬件设备采购明细，并获取采购合同、发行人入库单、出库单等，核查项目成本中硬件采购核算的准确性，以及采购背景的真实性及合理性。核查项目成本中人工成本对应的工时记录，与实际实施的项目周期进行对比分析。获取项目成本中的技术服务和软件的采购合同台账和服务验收单，核查项目成本中技术服务和软件采购核算是否准确，采购背景是否真实、合理。获取项目成本中其他费用的明细，并采用抽样方式检查相关的发票、付款等单据，核查是否真实、准确。经核查，发行人项目成本中硬件设备及软件、技术服务采购金额核算准确，采购背景真实，与发行人主营业务及项目需求相匹配。

8、获取发行人编制的主要项目的《项目执行情况表》，核查发行人对主要项目的跟踪情况及对合同签订可行性的记录情况。访谈相关项目负责人，了解发行人跟踪项目进度的具体措施。经核查，发行人持续、及时跟踪项目进展，具备

确保合同签订可行性的内控措施。

12、关于现金流量

根据申报材料：（1）2019 年、2020 年销售商品、提供劳务收到的现金金额大于营业收入金额；（2）报告期各期末应付暂收款分别为 130.04 万元、518.53 万元和 969.04 万元，2020 年末应付暂收款主要为员工报销款和代收代付款项；（3）2019 年公司采购大额电子设备，2020 年采购大额软件使用权。

请发行人根据《招股说明书准则》第 78 条的规定补充披露报告期经营活动产生的现金流量净额与净利润存在较大差异的影响因素。

请发行人说明：（1）2019 年、2020 年销售商品、提供劳务收到的现金大于营业收入的原因；（2）代收代付款项的内容、金额；（3）报告期内采购大额电子设备、软件使用权的原因及具体用途，主要供应商及采购金额。

请保荐机构、申报会计师对上述事项进行核查，并发表明确意见。

【回复】

（1）请发行人根据《招股说明书准则》第 78 条的规定补充披露报告期经营活动产生的现金流量净额与净利润存在较大差异的影响因素。

发行人已按要求在《招股说明书》“第八节 财务会计信息与管理层分析”之“十二、偿债能力、流动性与持续经营能力分析”之“（五）现金流量分析”之“1、经营活动产生的现金流量”对相关情况进行了补充披露，具体如下：

单位：万元

	2021 年 1-6 月	2020 年	2019 年	2018 年
1) 将净利润调节为经营活动现金流量：				
净利润	-2,033.94	4,229.58	162.63	331.91
加：资产减值准备	218.99	793.05	327.23	555.19
固定资产折旧、油气资产折耗、生产性生物资产折旧	494.58	956.20	323.71	276.85
使用权资产折旧	57.52	-	-	-
无形资产摊销	74.54	95.31	92.52	92.69
长期待摊费用摊销	37.20	75.39	72.21	2.00
处置固定资产、无形资产和其他长期资产的损失（收益以“-”号填列）	-	0.69	0.48	-

固定资产报废损失（收益以“－”号填列）	-	18.51	1.56	0.05
公允价值变动损失（收益以“－”号填列）	-	-	-	-
财务费用（收益以“－”号填列）	81.34	241.58	218.69	157.02
投资损失（收益以“－”号填列）	-273.20	-182.64	-331.61	-107.75
递延所得税资产减少（增加以“－”号填列）	-31.20	-129.34	-48.01	-68.60
递延所得税负债增加（减少以“－”号填列）	-	-	-	-
存货的减少（增加以“－”号填列）	-1,511.70	-535.47	-942.75	640.57
经营性应收项目的减少（增加以“－”号填列）	1,235.64	624.76	417.97	-5,885.37
经营性应付项目的增加（减少以“－”号填列）	-1,688.62	3,422.10	3,803.43	-1,405.91
其他	-	-	-	-
经营活动产生的现金流量净额	-3,338.87	9,609.73	4,098.06	-5,411.35

报告期内，公司经营活动产生的现金流量净额分别为-5,411.35 万元、4,098.06 万元、9,609.73 万元和-3,338.87 万元，净利润分别为 331.91 万元、162.63 万元、4,229.58 万元和-2,033.94 万元，差异分别为-5,743.26 万元、3,935.43 万元、5,380.15 万元和-1,304.93 万元。

①2018 年度差异

2018 年度公司净利润与经营活动产生的现金流量净额的差异为-5,743.26 万元，主要原因系公司业务拓展，应收账款等经营性应收项目较上一会计年度增加 5,885.37 万元所致。同时公司加强经营性现金流的管理，积极调整供应商预付账款情况，导致应付账款等经营性应付项目有所减少。

②2019 年度差异

2019 年度公司净利润与经营活动产生的现金流量净额的差异为 3,935.43 万元，主要原因系公司经营性应付项目增长所致：

A、2019 年公司新签业务合同金额为 23,925.87 万元，同比增长率为 31.68%，因此在建项目及合同首付款增加，导致预收款项较上一会计年度增加 2,500.20 万元；

B、公司在 2019 年调整了员工薪资结构与发放制度，因此在年末计提了年

年终奖未发放，导致期末应付职工薪酬增加 475.47 万元；

C、因业务拓展，2019 年公司员工报销款及因网络靶场系列产品、网络安全竞赛服务业务导致的代收代付款增加，导致公司其他应付款增加 399.52 万元。

③2020 年度差异

2020 年度公司净利润与经营活动产生的现金流量净额的差异为 5,380.15 万元，主要原因如下：

A、公司经营性应付项目较上一会计年度增长了 3,422.10 万元。

2020 年公司新签业务合同金额为 40,783.89 万元，同比增长 70.46%，首付款增加，导致期末预收款项及合同负债增加 2,115.88 万元；同时由于业务拓展，公司采购有较大幅度增加，因此导致应付账款增加 766.38 万元。

B、计提减值准备为 793.05 万元。

公司在 2020 年针对预计无法收回的应收款项进行了单项计提减值准备，因此导致 2020 年信用减值损失增加 500.17 万元；对于合同暂未签订的停滞项目对应的存货计提了跌价损失，因此导致资产减值损失增加 292.87 万元。

C、固定资产计提折旧为 956.20 万元。

公司工程实验室项目已于 2019 年达到预定可使用状态后转为固定资产，2020 年公司对其按照年限平均法计提了折旧，因此导致 2020 年公司固定资产计提折旧相较前一会计年度有所上升，本期计提折旧金额为 956.20 万元。

④2021 年 1-6 月份差异

2021 年 1-6 月度公司净利润与经营活动产生的现金流量净额的差异为 -1,304.93 万元，主要原因如下：

A、公司承接业务，项目建设导致人员成本归集增加，硬件、分包等采购成本归集增加，因而导致存货增加 1,511.70 万元。

B、因公司加大催款力度，当期应收账款回款提高，导致经营性应收项目减少 1,235.64 万元。

C、由于公司薪酬结构影响，本期发放了 2020 年计提的未发放奖金，导致期末应付职工薪酬下降；同时公司加强财务管理，对未支付的员工报销款进行了支付，期末其他应付款减少，因此导致经营性应付项目减少 1,688.62 万元。

请发行人说明：

(1)2019 年、2020 年销售商品、提供劳务收到的现金大于营业收入的原因;

2019 年公司销售商品、提供劳务收到的现金为 19,638.03 万元,营业收入为 16,308.54 万元;2020 年公司销售商品、提供劳务收到的现金为 33,976.91 万元,营业收入为 29,164.20 万元;2021 年 1-6 月销售商品、提供劳务收到的现金为 10,011.20 万元,营业收入为 8,136.08 万元,差异分别为 3,329.49 万元、4,812.72 万元和 1,875.13 万元,主要原因如下:

①2019 年差异原因

A、销售商品、提供劳务收到的现金金额为含税金额,营业收入为不含税金额。

2019 年销售商品、提供劳务收到的现金为 19,638.03 万元,营业收入 16,308.54 万元,因增值税引起的税差约为 1,000 万元。

B、新签合同金额有较大增长,预收款项及合同负债金额增加。

2019 年公司新签业务合同金额为 23,925.87 万元,同比增长率为 31.68%。合同规定的货款结算方式多为分期支付,首期款往往在合同签订后进行支付。而合同签订与项目完工并经由甲方验收,从而达到可以确认收入的状态之间具有一定的周期,因此公司 2019 年年末预收款项及合同负债有所增长,期末同比增加额为 2,500.20 万元。

②2020 年差异原因

A、销售商品、提供劳务收到的现金金额为含税金额,营业收入为不含税金额。

2020 年销售商品、提供劳务收到的现金为 33,976.91 万元,营业收入 29,164.20 万元,因增值税引起的税差约为 2,000 万元。

B、新签合同金额有较大增长,预收款项及合同负债金额增加。

2020 年公司新签业务合同金额为 40,783.89 万元,同比增长 70.46%,期末预收款项及合同负债的同比增加额为 2,115.88 万元。

C、2020 年应收账款回款情况较好。

2019 年末与 2020 年末公司应收账款账面余额分别为 10,978.56 万元和 9,997.65 万元,期末与期初差额为 959.07 万元,公司加大催收力度,且公司重大项目网络安全科技馆项目回款已超过 80%,因此应收账款当年回款情况较好。

③2021 年 1-6 月差异原因

2021 年 1-6 月差异主要系增值税与应收账款回款较好所致。

A、本期销售商品、提供劳务收到的现金为 10,011.20 万元，营业收入 8,136.08 万元，因增值税引起的税差约为 700.00 万元。

B、本期末公司应收账款账面余额为 9,101.08 万元，期初为 9,997.65 万元，因应收账款回款导致差额为 896.57 万元。

(2) 代收代付款项的内容、金额；

报告期内公司其他应付款分别为 133.04 万元、524.65 万元、975.39 万元和 357.01 万元，其中应付暂收款及往来款分别为 130.04 万元、518.53 万元、969.04 万元和 350.90 万元，其中应付暂收款的明细情况如下：

单位：万元

类别	2021 年 6 月末		2020 年末		2019 年末		2018 年末	
	金额	占比	金额	占比	金额	占比	金额	占比
社保、公积金等	63.45	18.08%	60.41	6.23%	47.67	9.19%	58.11	44.69%
员工报销款	131.09	37.36%	508.47	52.47%	387.46	74.73%	56.89	43.75%
代收代付	6.12	1.71%	107.49	11.09%	69.60	13.42%	-	-
往来款	150.24	42.82%	292.66	30.20%	13.79	2.66%	15.04	11.56%
合计	350.90	100%	969.04	100%	518.53	100%	130.04	100%

公司报告期内应付暂收款主要为员工报销款项、代收代付和社保、公积金等，合计占应付暂收款的比例为 88.44%、97.34%、69.80%和 57.15%。

公司报告期内代收代付的款项为：

①根据《中华人民共和国社会保险法》和《住房公积金管理条例》等法律法规要求，公司应付暂未支付的及代扣员工个人部分的社会保险费和住房公积金；

②根据相关协议的约定公司代收代付员工应予缴纳给北京市海淀区保障性住房发展有限公司保障房租赁款、代收代付学员的 CISP 考试报名费、代收代付成都天府新区投资集团有限公司的赛事奖金。

(3) 报告期内采购大额电子设备、软件使用权的原因及具体用途，主要供应商及采购金额。

一、采购大额电子设备

公司 2018 年至 2021 年 6 月末固定资产中电子设备账面原值分别为 853.02

万元、2,933.48 万元、2,832.54 万元和 2,948.47 万元，2019 年末电子设备增长较多，主要系在建工程中工程实验室项目达到预定可使用状态后转为固定资产所致。

2017 年公司开始建设工程实验室，实际支出含税金额 3,028.51 万元，其中财政拨款 895.00 万元，自筹资金 2,133.51 万元。2019 年 12 月，工程实验室项目已全部实施完成，达到预定可使用状态，截至 2019 年 12 月 31 日公司已将其转固。

2019 年工程实验室项目变动情况如下所示：

单位：万元

工程名称	自筹资金	财政拨款	实际支出	其中：转入固定资产
北京市工程实验室创新能力建设项目	2,133.51	895.00	3,028.51	2,028.80

工程实验室项目的主要供应商及采购金额如下表所示：

单位：万元

序号	供应商	采购类型	采购金额	用途
1	北京坤元和讯技术有限公司	软件	422.47	用于实验室内部阻止非法用户的侵入、加强网络数据处理能力、访问控制等
2	石家庄彰浩商贸有限公司	软件	335.98	用于实验室内部阻止非法用户的侵入、各类请求内容检测和验证、防御 APT 威胁、定位漏洞等
3	神州网云（北京）信息技术有限公司	软件	239.32	用于实验室内部主机检查、为众测平台提供知识库、漏洞检测分类修复等
4	安徽云探索网络科技有限公司	软件	180.11	用于实验室设备恶意代码检测、系统加固、运行状态监控和主机管控等
5	北京英信未来科技有限公司	硬件	171.44	实验室支持设备（服务器、硬盘）
6	北京金睛云华科技有限公司	软件	162.39	为实验室提供风险样本和威胁情报、发现 APT 攻击等
7	广州锦行网络科技有限公司	软件	155.34	用于验证发现可疑高危恶意代码变种，发现其特征和危险行为
8	北京天智恒仪教育科技有限公司	软件	97.09	检测缺陷、发现实验室平台中源代码开发中的问题
合计			1,764.14	

二、采购大额软件使用权

公司 2018 年至 2021 年 6 月末无形资产原值分别为 467.04 万元、467.04 万元、1,082.79 万元和 1,088.26 万元，2020 年末增长较多系外购管理软件、财务软

件和数据库等所致。

2020 年主要外购软件情况如下所示：

单位：万元

序号	软件名称	购入时间	供应商	无形资产购入金额	用途
1	奥联软件系统	2020/12/18	深圳奥联信息安全技术有限公司	267.26	研发部自用软件：加密、安全传输软件，用于提高密钥及数据安全性
2	犇众移动应用隐私检测软件	2020/12/31	上海犇众信息技术有限公司	103.54	公司内部使用的软件，用于对客户端设备进行检测，发现和定位已知和未知恶意代码和安全风险，检测隐藏型恶意软件
3	犇众盘古手机取证软件	2020/12/31	上海犇众信息技术有限公司	71.68	公司内部使用的软件，用于服务端对客户端设备进行取证分析，了解客户端设备在传输、渗透、安装、控制等行为，形成身份数据词典进行综合处置和调查取证
4	金蝶系统	2020/3/31	北京金蝶云创软件技术有限公司	55.82	公司内部使用的软件，金蝶 ERP 系统：费用报销、项目、预算、供应链业务模块、财务模块使用
5	Windows 群控系统	2020/8/29	北京信安天途科技有限公司	49.50	公司内部使用的软件，为互联网违法犯罪线索业务提供分布式爬虫及隐蔽通信技术支持
6	Android 系统群控控件开发	2020/11/10	北京志华空间科技有限公司	39.60	公司内部使用的软件，为互联网违法犯罪线索业务提供分布式爬虫及隐蔽通信技术支持
7	多跳 VPN 系统开发	2020/9/1	北京凌仕科技有限公司	24.75	公司内部使用的软件，为互联网违法犯罪线索发现提供分布式爬虫及隐蔽通信技术支持
合计				612.15	-

以上软件主要为加密软件及办公软件等，因公司日常研发及管理需求而采购，不存在将研发支出资本化并确认为无形资产的情形，无形资产确认符合相关会计准则。

【核查程序】

1、获取并检查发行人编制的现金流量表，分析经营活动产生的现金流量净额与净利润差异的主要项目，通过访谈总经理、财务总监等管理人员确认变动的原因；

2、对发行人 2019 年、2020 年“销售商品、提供劳务收到的现金”项目的具体情况进行检查，并与财务报表相关科目的变化进行相互勾稽；结合发行人收入明细情况、项目回款情况等信息，对公司 2019 年、2020 年销售商品、提供劳务收到的现金大于营业收入的原因进行分析；

3、获取并检查发行人报告期内的代收代付款项的明细信息，了解上述款项的实际业务内容；

4、获取并检查发行人报告期内电子设备、软件使用权的采购清单，访谈总经理、采购总监、财务总监等管理人员，了解上述资产采购的原因及具体用途；获取并检查报告期内电子设备、软件使用权的预算资料、采购合同、验收入库单据、付款凭证等资料。

【核查结论】

经核查，保荐机构及申报会计师认为：

1、发行人已根据《招股说明书准则》第 78 条的规定在《招股说明书》中补充披露报告期经营活动产生的现金流量净额与净利润存在较大差异的影响因素；

2、发行人 2019 年、2020 年销售商品、提供劳务收到的现金大于营业收入的原因合理，与实际经营情况相符；

3、报告期内，发行人代收代付的款项主要为代收代付的员工社会保险费、住房公积金、代收代付的保障房租金等，未见异常的代收代付款项；

4、报告期内，发行人的电子设备、软件使用权采购均系基于公司日常的经营、研发需求，与实际经营情况相符。

13、关于其他

13.1、关于同行业公司入股发行人

根据申报材料，同行业公司或其关联方存在入股发行人的情形，其中奇安创投持有发行人 15.51%股权，启明星辰持有发行人 4.07%股权。

请发行人结合上述股东的入股背景、与公司主营业务或产品的关联，说明与

公司是否存在共同客户及相关客户的获取方式。

请保荐机构、发行人律师对上述事项进行核查，并发表明确意见。

【回复】

一、奇安创投和启明星辰安全及其关联方入股发行人的背景

奇安信、奇安创投、启明星辰投资和启明星辰安全入股发行人的原因及背景情况如下：

序号	时间和事项	股东名称	入股背景
1	2014年4月8日,永信至诚有限第四次增资(注册资本人民币1,000万元增加至1,058.9474万元)	启明星辰投资	启明星辰投资为启明星辰全资子公司。启明星辰投资长期看好公司业务发展,与公司协商后,对公司增资入股。
2	2014年8月28日,永信至诚有限第五次增资(注册资本由人民币1,058.9474万元增至1,176.61万元)	奇安信	奇安信看好公司业务发展,与公司协商后,对公司增资入股。
3	2014年12月15日,永信至诚有限第三次股权转让(启明星辰投资向启明星辰安全转让其出资额)	启明星辰安全	启明星辰安全为启明星辰投资全资子公司,为启明星辰二级子公司。启明星辰出于内部管理需要,调整对发行人的投资持股主体。
4	2015年9月10日,永信至诚有限第六次增资(注册资本由人民币1,176.61万元增至1,238.53万元)	奇安信	奇安信看好公司业务发展,与公司协商后,对公司增资入股。
5	2017年9月4日,永信至诚第一次增资(注册资本由3000万元增至3,150万元,其中奇安信认购110万股)	奇安信	奇安信看好公司的高速发展,与公司协商后,对公司增资入股。
6	2018年6月27日,永信至诚股权转让(奇安信向奇安创投转让545万股)	奇安创投	奇安创投当时系奇安信关联公司(自2021年4月29日起,奇安创投不再是奇安信关联公司),系私募股权基金公司,主要业务是股权投资及相关咨询服务。

二、奇安创投和启明星辰安全及其关联方与发行人主营业务或产品的关联

(一) 奇安创投及奇安信与公司主营业务或产品的关联

奇安创投的主要业务为股权投资及相关咨询服务,与发行人的主营业务分属

于不同领域，因此奇安创投与发行人的主营业务或产品不存在关联。

奇安信为奇安创投的有限合伙人，直接持有奇安创投 15.3716% 的份额，间接持有发行人 2.38% 的股份。奇安信的主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务。由于奇安信与发行人同属于网络安全行业，奇安信规模较大，产品范围较广，因此奇安信的主营业务和产品与发行人存在部分重叠，但发行人的主营业务和产品是通过独立发展和自主研发取得，与奇安信无关联。

奇安信产品中的网络安全实训平台、网络空间态势感知与协调指挥系统、网络流量传感器、日志收集与分析系统、网络安全体系规划设计服务及风险评估等服务与发行人提供的产品及服务有一定相似性。另外，奇安信的全资子公司山东安云信息技术有限公司的火种 CTF 平台、安全人才培养产品及服务等与发行人的网络安全竞赛服务、线上线下培训服务存在一定相似性。该等产品与发行人同类型产品的比较如下：

类别	发行人主要产品	奇安信相似产品	产品差异
网络靶场系列产品	春秋云境网络靶场平台	网络安全实训平台	根据数世咨询于 2020 年 7 月 23 日发布的《网络靶场能力指南》，发行人的春秋云境网络靶场在应用创新力和市场执行力维度均位列第一，奇安信的靶场产品在市场执行力维度位列第一。 1、发行人的春秋云境网络靶场平台包含了赛事演练、人才培养、智慧城市安全测试、案件线索追踪、业务模拟仿真、人工智能攻防、复杂业务安全推演、综合场景应用等多业务场景。2018 年 10 月 25 日，中科合创（北京）科技成果评价中心（科技部有关部门批准成立的全国第一家第三方专业科技成果评价机构）组织院士等专家对公司的“城市网络靶场构建技术及应用”进行集中评定，认定“该项目达到国内领先水平”。公司的“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获 2019 年度北京市科学技术奖（科学技术进步奖）一等奖。 2、奇安信的网络安全解决方案包括实训、攻防竞赛、实战演练、科研测试等内容。
安全管控与蜜罐产品	春秋云阵新一代蜜罐系统	-	根据数世咨询于 2020 年 12 月发布的《蜜罐诱捕市场指南》，发行人的蜜罐产品在市场执行力和应用创新力维度均位于前列，奇安信并无此类产品进入该指南的点阵图。

	春秋云势网络安全态势感知与处置平台	网络空间安全态势感知与协调指挥系统	发行人的春秋云势网络安全态势感知与处置平台能够利用大数据、人工智能融合分析和处理各类安全设备和探针数据，发现高持续性网络安全威胁，并强调高处置流程（包括指挥调度、流程监管及数字化留痕）和对监测结果的跟踪管理。 奇安信网神网络空间安全态势感知与协调指挥系统支撑监管机构开展等级保护、监段检查、威胁通报、追踪溯源、侦查调查、信息共享、重大活动安保、应急协调指挥等核心工作。
安全工具类产品	流量监测、数据分析、业务支撑、安全辅助类产品	网络流量传感器、日志收集与分析系统	1、流量监测类产品：发行人的流量监测类产品能够发现流量中被加密或进行伪装的数据信息，通过解密和还原后，就被隐藏的数据信息进行分析。奇安信的网路流量传感器主要用于奇安信态势感知解决方案的网络流量采集设备，目前不单独销售。 2、数据分析类产品：双方产品类似，均用于发现网络违法线索，为监管部门进一步打击网络违法活动提供有价值的分析。 3、业务支撑类产品：发行人的业务支撑类产品是结合国家监管部门的需求定制开发的产品。根据公开途径查询，奇安信未就相关产品进行详细披露。 4、安全辅助类产品：发行人结合国家监管部门的需求定制开发安全辅助类产品，用于支持国家监管部门网络违法调查和违法行为取证工作。根据公开途径查询，奇安信未就相关产品进行详细披露。
安全防护系列服务	安全检测与评估、安全咨询、安全运维与分析处置、安全能力建设与评估	网络安全体系规划设计服务、风险评估服务等	发行人在提供安全防护系列服务的过程中，会利用到发行人自研的多种网络安全工具、蜜罐系统、网络靶场系统平台等完成数据采集、网络安全防御和对抗、数据取证、大数据分析、黑客攻击溯源反制、日志备份与检查、应急响应、安全加固等各类安全服务工作。奇安信未就相关产品进行详细披露。

网络安全竞赛服务	网鼎杯、强网杯、护网杯、巅峰极客等网络安全大赛	火种CTF（山东安云信息技术有限公司的竞赛平台）	发行人自 2014 年以来，支撑中央网信办、公安部、教育部、工信部、卫健委、国税总局、科技部等部委和单位主办或指导的超过 320 场网络安全演练，服务人数超过 38 万人次。包括：公安部主导的“网鼎杯”、中央网信办指导的“强网杯”、工信部主办的“全国工业互联网安全技术技能大赛”、信息安全重点实验室主办的“RHG 机器人网络安全大赛”等一系列重大的网络安全赛事和演练活动。 根据火种CTF网站显示的赛事信息，火种CTF自 2017 年开始举办网络安全赛事，主要赛事包括：（1）高校竞赛（山东理工大学、南通大学、中国药科大学、北华大学、潍坊学院、西北农林科技大学、山东中医药大学等）；（2）企业竞赛（北京银行、安徽移动业支付系统、武汉船院、中国宝武、山东电力网络）；（3）政府竞赛（内蒙古教育厅、云南公安、淮北公安、海南省公安、广东省广电网络、山东卫健委）。
其他服务	线上线下培训服务	子公司山东安云信息技术有限公司的安全人才培养产品及服务	线上线下培训服务的客户包括个人、企事业单位等，其中企事业单位客户包括南水北调中线信息科技有限公司、中国人寿保险股份有限公司、中国海洋石油集团有限公司、中信银行股份有限公司、厦门理工学院、海南政法职业学院、甘肃政法大学、网易（杭州）网络有限公司、中国民航信息网络股份有限公司、四川大学等。 根据企查查和天眼查显示的客户信息，山东安云信息技术有限公司服务的客户集中在山东省内，主要包括：山东省千佛山医院、山东省国土测绘院、济宁医学院附属医院、山东医学高等专科学校、济南职业学院、山东司法警官职业学院、德州市电子政务办公室、山东开放大学、滨州市中心医院、国网山西省电力公司、中电福富信息科技有限公司和中国海洋大学。

（二）启明星辰及其关联方与发行人主营业务或产品的关联

启明星辰安全为发行人的直接股东，持有发行人 4.07%的股份。启明星辰安全的主要业务为信息安全产品和专业安全业务、涉密业务。启明星辰安全为启明星辰投资全资子公司。

启明星辰投资持有启明星辰安全 100%的股权，其业务性质为项目投资与投资管理。启明星辰投资为启明星辰全资子公司。

启明星辰通过其二级全资子公司启明星辰安全持有发行人 4.07%的股份。启

明星辰是全面型的企业级网络安全厂商，为政企用户提供网络安全软件、软硬件一体化产品、平台化产品及安全运营与服务。由于启明星辰与发行人同属于网络安全行业，启明星辰规模较大，产品范围较广，因此启明星辰的主营业务和产品与发行人存在部分重叠，但发行人的主营业务和产品是通过独立发展和自主研发取得，与启明星辰无关联。

启明星辰产品中的网络安全靶场平台、云众可信平台的网络空间靶场、天阗欺骗防御系统、网络安全态势感知平台、天阗 APT 检测系列、泰合网络行为分析系统、业务支撑安全管理系统、网络空间安全学院及规划咨询服务、风险管理服务等服务与发行人提供的产品及服务有一定相似性，该等产品与发行人同类型产品的比较如下：

类别	发行人主要产品	启明星辰相似产品	产品差异
网络靶场系列产品	春秋云境网络靶场平台	网络安全靶场平台、云众可信平台的网络空间靶场	根据数世咨询于 2020 年 7 月 23 日发布的《网络靶场能力指南》，发行人的春秋云境网络靶场在应用创新力和市场执行力维度均位列第一。 1、发行人的春秋云境网络靶场平台包含了赛事演练、人才培养、智慧城市安全测试、案件线索追踪、业务模拟仿真、人工智能攻防、复杂业务安全推演、综合场景应用等多业务场景。2018 年 10 月 25 日，中科合创（北京）科技成果评价中心（科技部有关部门批准成立的全国第一家第三方专业科技成果评价机构）组织院士、行业专家等对公司“城市网络靶场构建技术及应用”进行集中评定，认定“该项目达到国内领先水平”。公司的“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获 2019 年度北京市科学技术奖（科学技术进步奖）一等奖。 2、启明星辰网络安全靶场平台通过网络安全仿真技术，快速、低成本的构建仿真网络环境，支撑用户在该环境中开展真实的大范围网络攻防演练、应急演练、培训教育，测试和评估网络环境安全和网络设施的薄弱环节，帮助用户预防未知威胁和攻击，提升安全防护能力。 3、根据启明星辰云众可信平台网站披露的信息，云众可信平台的核心产品包括网络空间靶场。但检索该网站，并未查询到有关网络空间靶场的信息。

安全 管控 与蜜 罐产 品	春秋云阵 新一代蜜罐 系统	天阗欺骗防御系 统	双方的产品均包括网络攻击捕获、网络攻击延缓、网络攻击溯源。 发行人的春秋云阵新一代蜜罐系统是借助于网络靶场系列产品的“平行仿真”技术构建更加接近真实业务的仿真能力（“高甜度”）进行欺骗式防御的蜜罐产品。 根据数世咨询于 2020 年 12 月发布的《蜜罐诱捕市场指南》，发行人的蜜罐产品在市场执行力和应用创新力维度均位于前列，启明星辰的产品并未出现在该指南中。
	春秋云势网 络安全态势 感知与处置 平台	网络安全态势感 知平台	发行人的春秋云势网络安全态势感知与处置平台能够利用大数据、人工智能融合分析和处理各类安全设备和探针数据，发现高持续性网络安全威胁，并强调高处置流程（包括指挥调度、流程监管及数字化留痕）和对监测结果的跟踪管理。 启明星辰的网络安全态势感知平台可支持资产采集、流采集、文件采集、包采集、漏洞采集、情报采集等能力，对设备、主机、日志、进程、服务等全要素信息的归并，帮助用户构造全方位、全天候态势感知系统的建设需求。
安全 工具 类产 品	流量监测、 数据分析、 业务支撑、 安全辅助类 产品	天阗 APT 检测系 列、泰合网络行 为分析系统、业 务支撑安全管理 系统	1、流量监测类产品：发行人的流量监测类产品能够发现流量中被加密或进行伪装的数据信息，通过解密和还原后，对被隐藏的数据信息进行分析。启明星辰未就天阗 APT 检测系列进行详细披露。 2、数据分析类产品：发行人的数据分析类产品使用实时关联规则引擎等，及时发现网络违法线索，为监管部门进一步打击网络违法活动提供价值分析。启明星辰未就泰合网络行为分析系统进行详细披露。 3、业务支撑类产品：发行人的业务支撑类产品是结合国家监管部门的需求定制开发的产品。启明星辰未就其相关产品进行详细披露。 4、安全辅助类产品：发行人结合国家监管部门的需求定制开发安全辅助类产品，用于支持国家监管部门网络违法调查和违法行为取证工作。启明星辰未就业务支撑安全管理系统进行详细披露。
安全 防护 系列 服务	安全检测与 评估、安全 咨询、安全 运维与分析 处置、安全	规划咨询服务、 风险管理服务、 运维与应急服 务、合规评价服 务、其他定制服	启明星辰未就相关产品进行详细披露。

	能力建设与评估等服务	务	
网络安全竞赛服务	网鼎杯、强网杯、护网杯、巅峰极客等网络安全大赛	-	根据公开途径查询，启明星辰目前无类似服务。
其他服务	线上线下培训服务	网络空间安全学院	公司 i 春秋实训平台目前其注册用户超过 89 万名，平台安全技术专家数量超过 700 人，课程超过 344 门。此外，平台建立了包含百度、阿里、腾讯、京东等八十多家互联网公司入驻的自有品牌 SRC（网络安全应急响应中心）部落。启明星辰网络安全空间学院包括安全运维课程体系、安全攻防课程体系、安全竞赛课程体系、认证类培训体系、安全管理课程体系、安全开发课程体系、安全管理课程体系、安全开发课程体系、安全管理课程体系、安全开发课程体系、安全管理课程体系、安全开发课程体系、安全管理课程体系、安全开发课程体系、安全管理课程体系、安全开发课程体系八大课程体系。

三、奇安创投和启明星辰与发行人是否存在共同客户及相关客户的获取方式

（一）奇安创投和奇安信与发行人是否存在共同客户及相关客户的获取方式

1、发行人与奇安创投的共同客户

奇安创投的主要业务为股权投资及相关咨询服务，发行人与奇安创投分属于不同业务领域。

2、发行人与奇安信的共同客户

在占发行人报告期内每年度确认收入 80% 的客户范围内，发行人与奇安信存在 37 名共同客户，报告期内，发行人向相关客户销售的收入占主营业务收入的比例分别为 14.00%、38.70% 和 13.50% 和 26.05%。

发行人与奇安信存在共同客户的原因是由于奇安信与发行人同属于网络安全行业，奇安信规模较大，产品范围较广，因此存在部分共同客户具有合理性，符合行业特性。

发行人与奇安信的共同客户为发行人独立拓展业务所取得，主要客户最早开始合作时间可追溯到 2011-2015 年，合同签订均为进行招投标程序后或双方谈判达成一致的结果，不存在客户来源于奇安信的情形。发行人与奇安信对下游客户的营销、产品供应及定价相互独立，交易定价公允，不存在通过共同客户进行利

益输送、利益捆绑、市场分割等情形。

（二）启明星辰与公司是否存在共同客户及相关客户的获取方式

1、发行人与启明星辰安全的共同客户

在占发行人报告期内每年度确认收入前 10 大客户范围内，发行人与启明星辰安全存在 6 名共同客户，报告期内，发行人向相关客户销售的收入占主营业务收入的比例分别为 9.58%、15.68%和 6.56%和 11.69%。

发行人与启明星辰安全存在共同客户的原因是由于启明星辰安全与发行人同属于网络安全行业，启明星辰安全规模较大，产品范围较广，因此存在部分共同客户具有合理性，符合行业特性。发行人与启明星辰安全的共同客户为发行人独立拓展业务所取得，最早开始合作时间可追溯到 2011 年，合同均为根据客户要求要求进行招投标程序或双方协商一致后签订，发行人不存在客户来源于启明星辰安全的情形，启明星辰安全不存在通过共同客户对发行人进行不当利益输送的情形。

2、发行人与启明星辰的共同客户

由于启明星辰为上市公司，其相关客户信息在年度报告中未披露相关信息以及涉及上市公司商业秘密，只同意给核对占发行人收入的前十大客户范围，未对全部客户进行核对。

报告期内，在占发行人各期确认收入前 10 大客户范围内，发行人与启明星辰不存在共同客户。

3、发行人与启明星辰投资的共同客户

经查询国家企业信用信息公示系统，发行人与启明星辰投资分属于不同业务领域。

由于启明星辰为上市公司，其相关客户信息在年度报告中未披露相关信息以及涉及上市公司商业秘密，且启明星辰（母公司）和启明星辰安全与发行人存在投资或业务关系，启明星辰体系内其他公司未与公司存在投资或者业务关系，因此只同意核对启明星辰（母公司）和启明星辰安全两个主体的客户重合关系。

【核查程序】

保荐机构和发行人律师核查过程如下：

1、取得发行人的工商资料和《股东调查表》；

- 2、取得奇安创投的营业执照、查询奇安信的经营范围；
- 3、查询奇安信招股说明书、奇安信官方网站、山东安云信息技术有限公司火种 CTF 竞赛平台网站，并就相关产品进行网络检索；
- 4、取得发行人报告期各期确认收入 80%的客户清单；
- 5、取得奇安信出具的有关与发行人共同客户的《说明函》，以核查在占发行人报告期内各期确认收入 80%的客户范围内发行人与奇安信存在的共同客户；
- 6、取得启明星辰安全的营业执照、查询启明星辰投资和启明星辰的经营范围；
- 7、查询启明星辰 2018 至 2020 年度年度报告、2021 年半年度报告，启明星辰官方网站、启明星辰云众可信平台网站，并就相关产品进行网络检索；
- 8、取得启明星辰和启明星辰安全出具的有关与发行人共同客户的《说明函》，以核查在占发行人报告期内各期确认收入前 10 大客户范围内发行人与启明星辰和启明星辰安全存在的共同客户。

【核查意见】

经核查，保荐机构及发行人律师认为：

- 1、发行人与奇安创投分属于不同业务领域；
- 2、经比对占发行人报告期内各期确认收入 80%的客户清单，发行人与奇安信存在共同客户。其原因是奇安信与发行人同属于网络安全行业，奇安信规模较大，产品范围较广，因此存在部分共同客户具有合理性，符合行业特性。发行人与奇安信的共同客户为发行人独立拓展业务所取得，不存在客户来源于奇安信的情形。发行人与奇安信对下游客户的营销、产品供应及定价相互独立，交易定价公允，不存在通过共同客户进行利益输送、利益捆绑、市场分割等情形；
- 3、发行人与启明星辰投资分属于不同业务领域；
- 4、经比对占发行人报告期内各期确认收入前 10 大客户清单，发行人与启明星辰不存在共同客户，与启明星辰安全存在共同客户的原因是启明星辰安全与发行人同属于网络安全行业，启明星辰安全规模较大，产品范围较广，因此存在部分共同客户具有合理性，符合行业特性。发行人与启明星辰安全的共同客户为发行人独立拓展业务所取得，发行人不存在客户来源于启明星辰安全的情形，启明星辰安全不存在通过共同客户对发行人进行不当利益输送的情形。

13.2、关于股东信息披露专项核查

根据《股东信息披露专项核查报告》，相关中介机构未就股东适格性发表明确意见。

请中介机构按照《关于科创板落实首发企业股东信息披露监管相关事项的通知》，完善核查报告，并发表明确意见。

【回复】

具体详见《股东信息披露专项核查报告》之“四、关于股东适格性”。相关核查程序和意见如下：

【核查程序】

针对发行人股东适格性情况，保荐机构和发行人律师履行了如下核查程序：

1、查验直接股东中法人股东、合伙企业股东的：

- （1）《机构股东调查表》；
- （2）《营业执照》及《公司章程》/《合伙协议》；
- （3）入股发行人的《验资报告》以及价款支付凭证；
- （4）企查查企业信用报告；
- （5）通过企查查进行股权穿透核查；

2、登录中国证券投资基金业协会网站查询发行人各私募投资基金股东的备案情况及私募投资基金管理人的登记情况；

3、查验直接股东中自然人股东的：

- （1）身份证复印件；
- （2）《自然人股东调查表》；
- （3）通过企查查查询其对外投资和任职情况，匹配其出资能力；

4、通过企查查进行股权穿透核查，按照穿透至自然人、上市公司（含境外上市公司）、新三板挂牌公司、国有控股或管理主体（含事业单位、国有主体控制的产业基金等）、集体所有制企业、境外政府投资基金、大学捐赠基金、养老基金、公益基金、公募资产管理产品、境外公司的原则进行股权穿透，并取得穿透背后间接自然人股东的身份证复印件、《自然人股东调查表》以及相关承诺文件；

5、根据《关于提供证监会系统离职人员信息查询比对服务的通知》的规定，向中国证券监督管理委员会北京监管局提交证监会系统离职人员信息查询申请，取得查询数据；

6、查阅发行人的股东名册，各中介机构出具的声明，董事、监事及高级管理人员填写的《董监高调查问卷》；

7、取得本次发行上市的中介机构及其负责人、高级管理人员、经办人员的身份证信息，与发行人直接及间接股东信息进行比对；

8、查验发行人出具的《股东信息披露承诺函》。

【核查意见】

经核查，保荐机构和发行人律师认为：

1、直接或间接持有发行人股份的主体具备法律、法规以及规范性文件规定的股东资格；

2、发行人股东与本次发行中介机构及其负责人、高级管理人员、经办人员不存在亲属关系、关联关系、委托持股、信托持股或其他利益输送安排；

3、发行人股东不存在以发行人股权进行不当利益输送的情况；

4、发行人已向保荐机构提交了《股东信息披露承诺函》符合《监管规则适用指引—关于申请首发上市企业股东信息披露》第二条的要求；

5、发行人股东不存在股权架构为两层以上且为无实际经营业务的公司或有限合伙企业，发行人股东入股价格均系结合当时实际入股背景由相关各方协商一致确定，与同次入股发行人的其他投资人入股价格相同，具有合理性，入股价格不存在明显异常，符合《监管规则适用指引—关于申请首发上市企业股东信息披露》第五条的要求；

6、发行人股东中的私募投资基金等金融产品已按照《中华人民共和国证券投资基金法》《私募投资基金监督管理暂行办法》《私募投资基金管理人登记和基金备案办法（试行）》等相关规定分别完成了私募基金备案和私募基金管理人登记程序，已经纳入国家金融监管部门的有效监管。

13.3、关于注销关联方

根据招股说明书，发行人曾持股 40%的北京果实春秋教育科技有限公司于 2018 年 5 月注销，报告期内曾是即刻点石子公司的广西永信于 2020 年 3 月份注

销。

请发行人说明上述子公司注销的原因，报告期内是否存在违法违规情形。

请保荐机构、发行人律师对上述事项进行核查，并发表明确意见。

【回复】

一、北京果实春秋教育科技有限公司与广西永信至诚信息科技有限公司注销的原因

（一）北京果实春秋教育科技有限公司

根据对北京果实春秋教育科技有限公司（以下简称“果实春秋”）原法定代表人肖元华和原股东王英键的访谈，设立果实春秋主要是为运营基于教育部“校盾计划”发展起来的有关业务。由于该等业务计划后续未能落实，因此果实春秋设立后未实际开展业务，故股东决定注销果实春秋。在果实春秋存续期间，各股东未进行实缴出资，也未聘用员工。

（二）广西永信至诚信息科技有限公司

公司设立广西永信主要是为拓展广西业务。广西永信设立后，该等市场拓展计划未实际落实，出于公司经营和内部管理需要，股东即刻点石决定注销广西永信。在广西永信存续期间，股东未进行实缴出资，也未聘用员工。

（三）福建函谷信息科技有限公司

福建函谷报告期内为发行人子公司即刻点石的控股子公司，已于 2021 年 12 月 16 日注销。即刻点石与后生仔（福建）实业有限公司共同设立福建函谷主要是为了拓展福建业务。福建函谷设立后，该等市场拓展计划未实际落实，出于公司经营和内部管理需要，股东即刻点石决定注销福建函谷。在福建函谷存续期间，未实际开展业务，也未聘用员工。

二、报告期内是否存在违法违规情形

报告期内，北京果实春秋教育科技有限公司与广西永信至诚信息科技有限公司均不存在违法违规情形。

国家税务总局大田县税务局均溪税务分局分别于 2021 年 4 月 3 日、2021 年 6 月 10 日作出《税务行政处罚决定书（简易）》（田税均溪简罚[2021]4 号、田税均溪简罚[2021]14 号），因福建函谷 2021 年 2 月 1 日至 2021 年 2 月 28 日、2021 年 4 月 1 日至 2021 年 4 月 30 日的个人所得税（工资薪金所得）未按期进

行申报，故对福建函谷分别作出罚款 100 元的处罚。福建函谷已缴纳罚款。除此之外，报告期内，福建函谷不存在违法违规情形。

【核查程序】

- 1、查阅果实春秋的工商档案和财务报表；
- 2、访谈果实春秋原法定代表人肖元华和原股东王英键，了解果实春秋的注销原因、报告期内是否存在违法违规情形等；
- 3、查阅广西永信的工商档案和对公活期存款交易明细报表；
- 4、访谈发行人相关负责人，了解广西永信的注销原因、报告期内是否存在违法违规情形等；
- 5、取得北海工业园区市场监督管理局出具的广西永信在存续期间未受到行政处罚的《证明》；
- 6、查阅福建函谷的工商档案和财务报表；
- 7、访谈发行人相关负责人，了解福建函谷的注销原因、报告期内是否存在违法违规情形等；
- 8、取得大田县市场监督管理局出具的福建函谷在存续期间不存在不良信用记录的《市场主体信用信息证明》；
- 9、取得国家税务总局大田县税务局出具的福建函谷税务事项均已结清的《清税证明》；
- 10、取得国家税务总局大田县税务局均溪税务分局分别于 2021 年 4 月 3 日、2021 年 6 月 10 日作出的《税务行政处罚决定书（简易）》（田税均溪简罚[2021]4 号、田税均溪简罚[2021]14 号）；
- 11、在国家企业信用信息公示系统、中国裁判文书网、中国执行信息公开网等网站查询，核查果实春秋、广西永信和福建函谷报告期内是否存在违法违规情形。

【核查意见】

经核查，保荐机构及发行人律师认为，报告期内，果实春秋和广西永信不存在违法违规行为。除国家税务总局大田县税务局均溪税务分局分别于 2021 年 4 月 3 日、2021 年 6 月 10 日作出的《税务行政处罚决定书（简易）》（田税均溪简罚[2021]4 号、田税均溪简罚[2021]14 号）外，报告期内，福建函谷不存在违

法违规情形。

13.4、关于信息披露豁免

根据申报材料，报告期内，发行人持有《涉密信息系统集成资质证书》《武器装备科研生产单位二级保密资格证书》。发行人依据相关规定，对涉密合同、涉密项目等相关涉密信息进行了脱密处理。发行人认为相关披露不涉及涉密信息，不涉及需要申请信息豁免披露的情形。

请保荐机构、发行人律师就发行人未按照《涉军企事业单位改制重组上市及上市后资本运作军工事项审查工作管理暂行办法》第三十五条办理涉密信息披露审查的依据是否充分进行核查，并发表明确意见。

【回复】

发行人不是《涉军企事业单位改制重组上市及上市后资本运作军工事项审查工作管理暂行办法》规定的涉军企事业单位，发行人本次公开发行股票并在科创板上市不适用《涉军企事业单位改制重组上市及上市后资本运作军工事项审查工作管理暂行办法》。发行人已披露的信息不涉及需要申请信息豁免披露的情形，发行人所披露的信息不违反国家相关保密规定。

一、发行人并非涉军企业，无须按 209 号文履行军工事项审查程序

《涉军企事业单位改制重组上市及上市后资本运作军工事项审查工作管理暂行办法》（科工计[2016]209 号，以下简称“209 号文”），根据 209 号文第二条规定，“涉军企事业单位，是指已取得武器装备科研生产许可的企事业单位。军工事项，是指涉军企事业单位改制、重组、上市及上市后资本运作过程中涉及军品科研生产能力结构布局、军品科研生产任务和能力建设项目、军工关键设备设施管理、武器装备科研生产许可条件、国防知识产权、安全保密等事项。”第三条规定，“本办法适用于国家国防科技工业局（以下简称国防科工局）对涉军企事业单位改制、重组、上市及上市后资本运作军工事项审查。军工事项外的其他事项，按照国家有关规定办理。”

根据《武器装备科研生产许可管理条例》和《武器装备科研生产许可实施办法》的规定，从事武器装备科研生产许可目录所列的武器装备科研生产活动的，应事先取得《武器装备科研生产许可证》。

发行人的业务不涉及“从事武器装备科研生产许可目录所列的武器装备科研

生产活动”，无需取得《武器装备科研生产许可证》，发行人也未取得《武器装备科研生产许可证》。因此根据 209 号文的相关规定，发行人不属于涉军企事业单位，无须按 209 号文履行军工事项审查程序。

二、发行人不涉及需要申请信息豁免披露的情形，所披露的信息不违反国家相关保密规定

209 号文第三十五条规定，“取得武器装备科研生产单位保密资格，但未取得武器装备科研生产许可的企事业单位实施改制、重组、上市及上市后资本运作，按有关规定办理涉密信息披露审查。”

上海证券交易所科创板在审企业北京谷数科技股份有限公司与发行人情况比较类似，其具有武器科研生产单位三级保密资格，未持有《武器装备科研生产许可证》。根据 2021 年 8 月 19 日披露的《关于北京谷数科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函的回复》，2021 年 8 月 2 日，北京市国防科学技术工业办公室出具了《关于北京谷数科技股份有限公司科创板上市的说明》（京军工函[2021]30 号），确认“你公司尚未从事列入武器装备科研生产许可目录范围内的武器装备科研生产活动，不在上市军工事项及特殊财务信息豁免披露的审查范围。建议你公司根据国家国防科工局相关规定，对涉军单位、项目、合同等相关涉密信息，进行脱密处理后披露。”

2021 年 12 月 20 日，北京市国防科学技术工业办公室出具了《关于为北京永信至诚科技股份有限公司出具相关说明的复函》（京军工函[2021]49 号），确认“北京永信至诚科技股份有限公司尚未从事列入武器装备科研生产许可目录范围内的武器装备科研生产活动，不在上市军工事项及特殊财务信息豁免披露的审查范围”。经电话咨询国家国防科技工业局，其建议发行人对相关涉密信息，进行脱密处理后披露。因此发行人对外披露的特殊财务信息应当由发行人保密部门组织进行保密审查，对外披露前应当采用代称、打包或者汇总等方式进行脱密处理。

根据《军工企业对外融资特殊财务信息披露管理暂行办法》（科工财审 2008[702]号）等法规的相关规定，军工企业涉密信息应采取脱密处理的方式进行披露，部分无法进行脱密处理或者进行脱密处理后仍存在泄密风险的信息，军工企业应向国家主管部门或证券交易所申请豁免披露。

发行人保密部门已针对招股说明书等申请文件中的涉及国家秘密的信息进行脱密处理和保密审查，确认招股说明书等申请文件中披露的信息不存在泄露国家秘密的情况，无需向国家主管部门或证券交易所申请豁免披露。

2021年9月16日，北京市国家保密局出具了相关文件，确认发行人自2019年6月取得武器科研生产单位二级保密资格以来，未发现其存在违反保密法律法规及因违反保密规定受到处罚的情况。

在证券交易所和证监会审核过程中，若后续的信息披露涉及军工涉密信息披露或国家保密信息披露的，发行人将对涉密信息作脱密处理后披露，若部分无法进行脱密处理或者进行脱密处理后仍存在泄密风险的信息，发行人将向证券交易所申请豁免披露。

综上，发行人不涉及需要申请信息豁免披露的情形，发行人保密部门已针对披露材料涉及国家秘密的信息进行保密审查及脱密处理，所披露的信息不违反国家相关保密规定。

【核查程序】

1、查阅《涉军企事业单位改制重组上市及上市后资本运作军工事项审查工作管理暂行办法》《军工企业对外融资特殊财务信息披露管理暂行办法》等规定；

2、检索公开披露信息中的相关案例；

3、电话咨询北京市国防科学技术工业办公室、国家国防科技工业局，核实发行人是否需要信息进行豁免披露审查，并取得北京市国防科学技术工业办公室出具的书面文件；

4、访谈发行人保密部门负责人，了解保密部门对本次发行申请文件的保密审查及脱密处理情况。

【核查意见】

经核查，保荐机构及律师认为：

1、发行人的业务不涉及“从事武器装备科研生产许可目录所列的武器装备科研生产活动”，未取得《武器装备科研生产许可证》，发行人不属于涉军企事业单位，无须按209号文履行军工事项审查程序；

2、发行人不涉及需要申请信息豁免披露的情形，发行人保密部门已经按照《军工企业对外融资特殊财务信息披露管理暂行办法》等要求对披露材料涉及国

家秘密的信息进行保密审查及脱密处理，所披露的信息不违反国家相关保密规定。

13.5、关于信息披露

请发行人：（1）严格按照《关于切实提高招股说明书（申报稿）质量和问询回复质量相关注意事项的通知》的规定，修改“重大事项提示”“风险因素”相关章节内容，按重要性进行排序，对相关风险因素作定量分析，包括但不限于公司业绩下滑甚至亏损风险、市场竞争风险等，删除“发行失败风险”“证券市场风险”等；（2）按照《关于切实提高招股说明书（申报稿）质量和问询回复质量相关注意事项的通知》出具欺诈发行股份购回承诺。

【回复】

（1）严格按照《关于切实提高招股说明书（申报稿）质量和问询回复质量相关注意事项的通知》的规定，修改“重大事项提示”“风险因素”相关章节内容，按重要性进行排序，对相关风险因素作定量分析，包括但不限于公司业绩下滑甚至亏损风险、市场竞争风险等，删除“发行失败风险”“证券市场风险”等；

发行人已按照《关于切实提高招股说明书（申报稿）质量和问询回复质量相关注意事项的通知》的规定，全面梳理了“重大事项提示”“风险因素”各项内容，对风险进行分类并按重要性进行排序，细化风险因素，使用定量或者针对性的定性提示，删除了“发行失败风险”“证券市场风险”。

（2）按照《关于切实提高招股说明书（申报稿）质量和问询回复质量相关注意事项的通知》出具欺诈发行股份购回承诺。

【回复】

一、公司及控股股东、实际控制人已重新单独出具欺诈发行股份购回承诺。

公司出具承诺如下：

“1、本公司保证本次公开发行股票并在上海证券交易所科创板上市不存在任何欺诈发行的情况；

2、如本公司不符合发行上市条件，以欺骗手段骗取发行注册并已经发行上市的，本公司将在中国证券监督管理委员会、上海证券交易所等有权部门确认后5个工作日内启动股份购回程序，购回本公司本次公开发行的全部新股，并承担与此相关的一切法律责任。”

控股股东、实际控制人出具承诺如下：

“1、本人保证本次公开发行股票并在上海证券交易所科创板上市不存在任何欺诈发行的情况；

2、如本公司不符合发行上市条件，以欺骗手段骗取发行注册并已经发行上市的，本人承诺在中国证券监督管理委员会、上海证券交易所等有权部门确认后5个工作日内启动股份购回程序，购回本公司本次公开发行的全部新股，并承担与此相关的一切法律责任。”

二、披露内容

公司已于招股说明书“第十节 投资者保护”之“五、发行人、股东、实际控制人、发行人的董事、监事、高级管理人员、核心技术人员以及本次发行的保荐人及证券服务机构等作出的重要承诺”之“（四）对欺诈发行上市的股份购回承诺”披露相关承诺如下：

“1、保证公司本次公开发行股票并在上海证券交易所科创板上市，不存在任何欺诈发行的情形。

2、如公司不符合发行上市条件，以欺骗手段骗取发行注册并已经发行上市的，本人/本公司承诺在中国证券监督管理委员会、上海证券交易所等有权部门确认后5个工作日内启动股份购回程序，购回本公司本次公开发行的全部新股，并承担与此相关的一切法律责任。”

13.6、关于媒体质疑

请保荐机构自查与发行人本次公开发行相关的重大媒体质疑情况，并就相关媒体质疑核查并发表意见。

【回复】

一、媒体质疑情况

自发行人取得上交所受理函以来，保荐机构持续关注媒体报道，经公开网络检索，已自查与发行人本次公开发行相关的媒体质疑情况。截至本回复签署之日，共有3篇媒体质疑报道，上述媒体质疑相关内容主要摘录招股说明书内容，发行人已进行充分披露和说明。保荐机构就相关媒体质疑进行了充分核查，认为上述媒体质疑不会影响发行人本次发行上市条件。相关质疑报道及媒体主要关注要点如下：

序号	日期	媒体	文章标题	媒体关注点
----	----	----	------	-------

1	2021/7/16	界面新闻	披着网络安全的外衣，做着教育培训的生意，永信至诚冲科创板含金量如何	1、科创属性不明显； 2、2020 年营收大幅增长、毛利率下降； 3、销售费用增长； 4、应收账款高且回款难。
2	2021/7/31	犀牛财经	永信至诚业绩不稳定，因存货数不符等遭处罚，涉软件著作权诉讼	1、业绩大幅波动； 2、关于行政处罚； 3、关于诉讼； 4、重营销轻研发。
3	2021/8/11	国际金融报	永信至诚“牛”了：前东家是竞争对手，却给它“送钱”又“送人”……	1、公司成立之初存在股权代持情况； 2、启明星辰与公司的“特殊”关系； 3、业绩波动较大。

二、保荐机构核查情况

上述媒体质疑相关内容主要摘录招股说明书内容，截至本回复签署之日，发行人已进行充分披露和说明；上述媒体质疑不会影响发行人本次发行上市条件。

14、保荐机构总体意见

对本回复材料中的发行人回复（包括补充披露和说明的事项），保荐机构均已进行核查，确认并保证其真实、完整、准确。

（本页无正文，为北京永信至诚科技股份有限公司《关于北京永信至诚科技股份有限公司首次公开发行股票并在科创板上市申请文件审核问询函的回复》之签章页）

北京永信至诚科技股份有限公司



发行人董事长声明

本人已认真阅读北京永信至诚科技股份有限公司本次审核问询函回复的全部内容，确认回复内容真实、准确、完整，不存在虚假记载、误导性陈述或者重大遗漏，并承担相应法律责任。

董事长：


蔡晶晶

北京永信至诚科技股份有限公司



2021年12月24日

（以下无正文，为《关于北京永信至诚科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函的回复报告》之保荐机构签字盖章页）

保荐代表人：

侯英刚
侯英刚

韩培培
韩培培



保荐人（主承销商）总经理声明

本人已认真阅读北京永信至诚科技股份有限公司本次审核问询函的回复报告的全部内容，了解报告涉及问题的核查过程、本公司的内核和风险控制流程，确认本公司按照勤勉尽责原则履行核查程序，审核问询函的回复报告不存在虚假记载、误导性陈述或者重大遗漏，并对上述文件的真实性、准确性、完整性、及时性承担相应法律责任。

总经理：


邓 舸

