启明星辰信息技术集团股份有限公司

公开发行可转换公司债券募集资金运用可行性分析报告（修订稿）

一、本次募集资金的使用计划

本次发行的募集资金总额（含发行费用）不超过 109,000.00 万元，募集资金扣除发行费用后，将投资于以下项目：

单位：万元

项目名称	项目总投资额	拟投入募集资金	自筹资金投入额
济南安全运营中心建设项目	9,200	5,700	3,500
杭州安全运营中心建设项目	28,000	13,500	14,500
昆明安全运营中心和网络安全培训中心建设项目	47,300	37,300	10,000
郑州安全运营中心和网络安全培训中心建设项目	50,500	37,500	13,000
补充流动资金	15,000	15,000	-
合计	**150,000**	**109,000**	**41,000**

在不改变募集资金投资项目的前提下，公司董事会可根据项目的实际需求，对上述项目的募集资金投入顺序和金额进行适当调整。

若本次发行实际募集资金净额低于拟投入项目的资金需求额，不足部分由公司自筹解决。募集资金到位之前，公司将根据项目进度的实际情况以自有资金或其它方式筹集的资金先行投入，并在募集资金到位后予以置换。

二、本次募集资金投资项目实施的背景

（一）中国网络安全政策密集发布，为行业发展营造了良好的环境

近年来，多项网络安全监管要求、推进产业发展和网络安全人才培养的法律法规和政策措施密集发布，为网络安全产业的发展营造了良好的环境。

2016 年，国家通过了新《网络安全法》，从法律层面明确提出国家实行网络安全等级保护制度，指出网络运营者应当按照网络安全等级保护制度的要求，制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任，并提出了相关设备的保护措施，尤其是对关键信息基础设施。2017 年 7 月 11 日，

国家互联网信息办公室发出《关键信息基础设施安全保护条例（征求意见稿）》明确规定，地市级以上人民政府应当将关键信息基础设施安全保护工作纳入地区经济社会发展总体规划，加大投入，开展工作绩效考核评价。等级保护制度的出台加大了各机构对于网络安全的重视。

工控安全事关经济发展、社会稳定和国家安全。近年来，随着信息化和工业化融合的不断深入，工业控制系统从单机走向互联，从封闭走向开放，从自动化走向智能化。在生产力显著提高的同时，工业控制系统面临着日益严峻的信息安全威胁。2016 年工信部为迎合产业发展需求，印发《工业控制系统信息安全防护指南》指导工业企业开展工控安全防护工作，成为国家网络和信息安全的重要组成部分，是推动中国制造 2025、制造业与互联网融合发展的基础保障。

随着云服务的普及，云安全问题凸显出来，备受国家关注。2017 年 3 月 30 日，国家电子政务外网管理中心办公室组织发布了《政务云安全要求》，该标准为指导全国各级政务部门开展政务云服务提供安全和管理依据，保证政务云服务的安全要求。对政务云监管严格要求催生了云安全市场。

国家在网络安全人才培养方面也出台了相应的支持政策。《网络安全法》从法律层面提出国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。2017 年 8 月 14 日，国家网信办在官网发布《一流网络安全学院建设示范项目管理办法》，提出在 2017 年至 2027 年实施一流网络安全学院建设示范项目，建成 4 至 6 所“国内公认、国际上具有影响力和知名度”的网络安全学院的目标。多项支持政策为企业开办网络安全培训学院提供了契机，也为校企合作、企企合作创造了条件。

（二）中国信息安全市场快速发展，服务市场增速更快

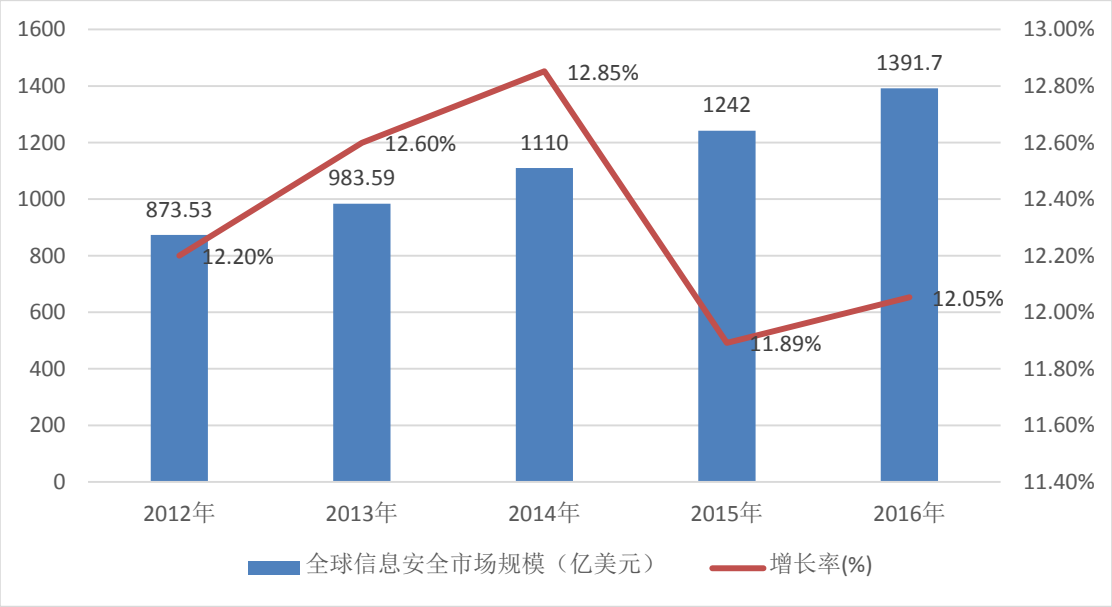
与全球信息安全市场相比，中国信息安全行业正处于快速成长期。信息安全需求从核心业务安全监控向全面业务安全保护扩展，从网络实施阶段的安全布置到网络运行过程的安全维护，安全需求正在向更高层次、更广范围延伸，安全服务的市场需求不断扩大。

1、全球信息安全市场快速发展，中国市场增速更快

近年来，全球网络威胁持续增长，网络罪犯在恶意代码和服务的开发、传播和使用上愈发趋于专业化，目的愈发趋于商业化，行为愈发组织化，手段愈发多

样化，造成的损失也随着范围的扩散而快速增多。持续增长的网络威胁促进全球信息安全产品的快速发展。2016 年，全球信息安全市场规模达到 1,391.7 亿美元，同比增长 12.05%，保持稳健增长的态势。

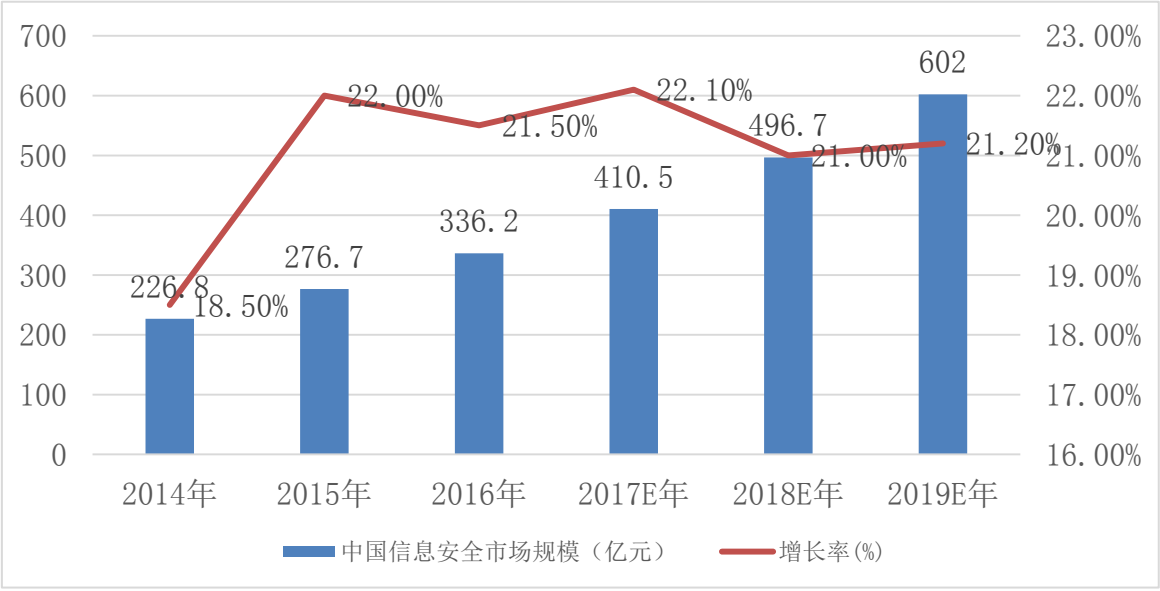
图 1 2012-2016 年全球信息安全市场规模及增长率



数据来源：赛迪顾问，2017 年

2016 年，中国的信息安全市场达到 336.2 亿元，同比增长 21.2%，高于全球增长率 12.05%，国内信息安全市场前景可观。据赛迪顾问预估，未来两年国内信息安全市场呈持续高速增长，增长率都保持在 20%以上。

图 2 2014 年-2019 年中国信息安全市场规模与增长率

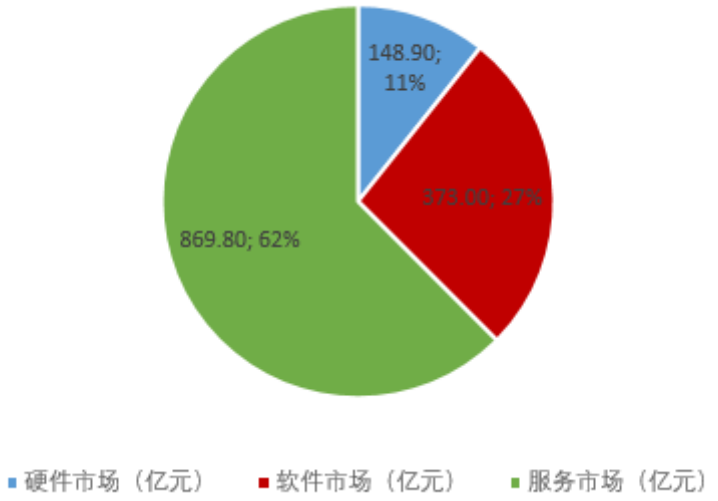


数据来源：赛迪顾问，2017 年（注：2017-2019 年的数据为赛迪顾问预测）

2、信息安全服务市场态势向好

信息安全产品包括三部分：硬件、软件和服务。在全球市场中，随着云安全和移动安全等新型领域安全的发展，安全服务化理念深入人心，安全服务和安全软件成为发展热点，2016 年分别占整个信息产品市场的 62%和 27%。

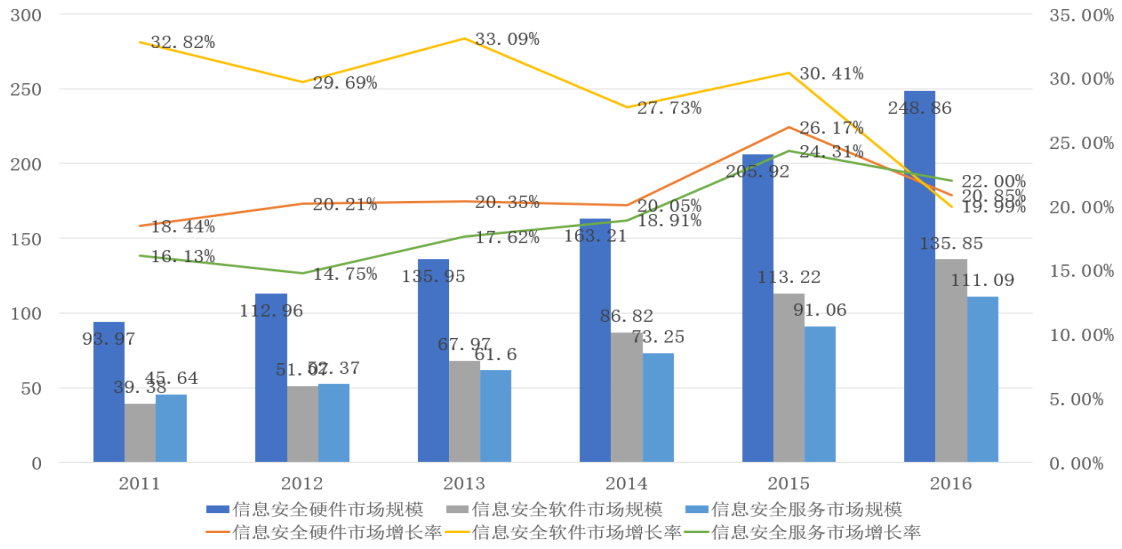
图 3 2016 年全球信息安全市场产品结构



数据来源：赛迪顾问，2017 年

目前中国信息安全市场仍是以硬件为主。由图 4 可见，虽然信息安全硬件市场占比最大，但是市场规模增长率持续下跌，由 2011 年的 32.82%下降到 2016 年的 19.99%。相反，服务市场表现出持续上升的势头，从 2011 年的 16.13%上升到 2016 年的 22%，增速高于信息安全产品市场，中国信息安全服务市场态势向好。

图 4 2010-2016 年中国信息安全产品市场发展现状



数据来源：赛迪顾问，2017 年

随着中国信息产业和网络技术的发展，传统的信息安全产品难以满足日益变化的复杂的网络空间，中国的信息安全产品行业必将向国际看齐，由硬件为主转换为服务为主。目前国内信息安全领域的重要企业，均在开展行业解决方案策划和推广工作，从产品导向型企业向服务导向型企业转变，以适应未来用户定制化服务和细分市场等发展趋势。

3、信息安全服务模式转型大步推进，正向网络安全运维模式过渡

由于信息安全行业的产品先众多，大到集团公司小到部门，都可能需要针对单个产品进行单独招标，并且为了防止一家独大，往往出现刻意分散招标的情况，导致信息安全行业出现小公司林立、市场集中度较为分散的格局，而由于分散招标，很难形成各种网安产品的立体联动防御和大数据分析，信息安全公司也很难提供有效的整体安全服务。但是随着大数据、云模式以及需求升级的三级推动，信息安全行业有望从当前的产品采购模式逐步向安全运维模式过渡，并且高壁垒决定了行业竞争格局走向集中。启明星辰建立城市安全运营中心，将自己二十多年的产品和技术积累优势发挥出来，为部门众多的政府和事业单位，提供统一的安全服务，形成自己的核心竞争优势。

（三）云计算、大数据、移动互联等技术的发展拓宽安全防护领域，为信息安全企业带来了挑战和机遇

由国家安全战略角度延伸到区域城市级安全环境来看，以智慧城市为核心承载体，大数据、物联网、移动互联、云计算普及的当前社会环境下，网络相关设备智能化、规模化、小型化、多样化的特点越发明显，伴生了网络空间复杂、网络环境多变、网络风险增高等安全方面的各种问题，成为影响社会经济健康发展的重要制约因素。

国家计算机网络应急技术处理协调中心日前发布的《2016 年中国互联网网络安全报告》中描述到：

- 高级持续性威胁常态化，我国面临的攻击威胁尤为严重；
- 针对工业控制系统的攻击日益增多，多起重要工业控制系统安全事件应引起重视；
- 大量联网智能设备遭受恶意程序攻击形成僵尸网络，被用于发起大流量 DDoS 攻击；
- 网站数据和个人信息泄漏屡见不鲜，衍生灾害严重；

- 移动互联网恶意程序趋利性更加明显，移动互联网黑色产业链已经成熟；
- 敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全。

总的来看，新技术环境下信息安全的要求更多、更高，传统的信息安全产品和服务难以满足市场的需求，对于整个信息安全行业来说，既是一项挑战也是一次机遇。

（四）政府在智慧城市建设中网络安全意识显著提升

在“互联网+”时代背景下的智慧城市建设高度集成了物联网、云计算、大数据等众多新形态的信息技术，这些都是实现城市职能智能化的基础，是一项复杂的大型系统工程，从传感感知层、通信传输层、应用层、智能分析处理等诸多层面存在安全风险和脆弱性，具有区别于传统网络时代特点的信息安全风险。一旦在信息安全防护上不能得到有效保证，可能造成城市管理职能出现混乱、隐私信息泄露、应急决策失误、各类事故频发乃至局部社会动荡的局面。

近几年，随着智慧城市的高速发展，与智慧城市相关的信息安全事件频发，长期维持在较高水平，引起了国家高度关注。2014 年 8 月，八部委联合发布的智慧城市建设的纲领性文件《关于促进智慧城市健康发展的指导意见》中明确了要完善管理机制，“要加快研究制定智慧城市建设的标准体系”。2015 年 11 月国家标准委联合中央网信办及国家发展改革委印发《关于开展智慧城市标准体系和评价指标体系建设及应用实施的指导意见》(国标委工二联〔2015〕64 号，以下简称《意见》)。《意见》明确到 2017 年，将完成智慧城市总体、支撑技术与平台、基础设施、建设与宜居、管理与服务、产业与经济、安全与保障 7 个大类 20 项急需标准的制订工作，到 2020 年累计完成 50 项左右的标准。

三、本次募集资金投资项目实施的必要性

（一）该项目是保障政府和企业信息安全的需要

随着信息技术和信息产业的迅猛发展，信息技术的应用领域逐渐从小型业务系统向大型、关键业务系统扩展，越来越多的政府机关和企事业单位建立了自己的信息网络，并与 Internet 相联，信息系统的基础性、全局性作用日益增强。作为保障和维护信息系统安全的重要工具和手段，信息安全产品在信息系统的地位越来越重要。近几年来，针对政府、科研机构、关键基础设施的窃密、破坏行为层出不穷，APT 攻击、木马远程控制、Oday、社会工程攻击、网络钓鱼等高级威胁

严重影响到政府信息安全。

棱镜门事件以后，国务院新闻办互联网新闻研究中心发布了一份名为《美国全球监听行动纪录》的报告显示，我国几乎所有的电子重要信息均暴露在美国的监控之下，国家安全形势严峻，提升安全投入刻不容缓。

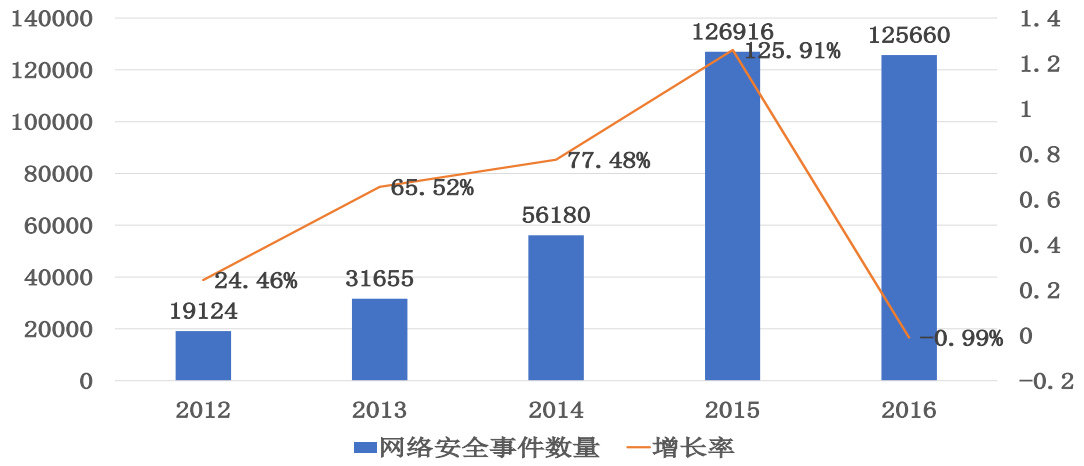
图 5 5 美国针对中国及全球的监视行为

《美国全球监听行动纪录》列出的美国对全球与中国的监控行为
每天收集全球各地近50亿条移动电话记录。《南华早报》援引斯诺登的话说：“美国国家安全局无所不用其极，非法入侵中国主要电信公司等手段，窃取用户的手机数据。
窥探德国现任总理默克尔手机长达十多年（此外，美国国家安全局2009年还针对122名外国领导人实施监控）
秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络，窃取了数以亿计的用户信息
多年来一直监控手机应用程序，抓取个人数据
针对中国进行大规模网络攻击，并把中国领导人和华为公司列为目标（攻击的目标包括商务部、外交部、银行和电信公司等。《明镜》周刊称，美国的监控目标还包括数位中国前任国家领导人和多个政府部门及银行。此外，美国国家安全局的一个特别小组成功渗透进了华为公司的计算机网络，并复制了超过1400个客户的资料和工程师使用的内部培训文件，该局人员不但窃取了华为的电子邮件存档，还获取了个别华为产品的源代码
美国的监听行动，涉及到中国政府和领导人、中资企业、科研机构、普通网民、广大手机用户

资料来源：《美国全球监听行动纪录》

当前随着我国互联网普及，联网终端与系统数量高速增长，相对应的网络安全投入严重不足，导致近几年国内安全事件呈井喷式增长，2015 年增长约 126%，突破 12 万件，给企业和整个社会带来巨大的经济损失。

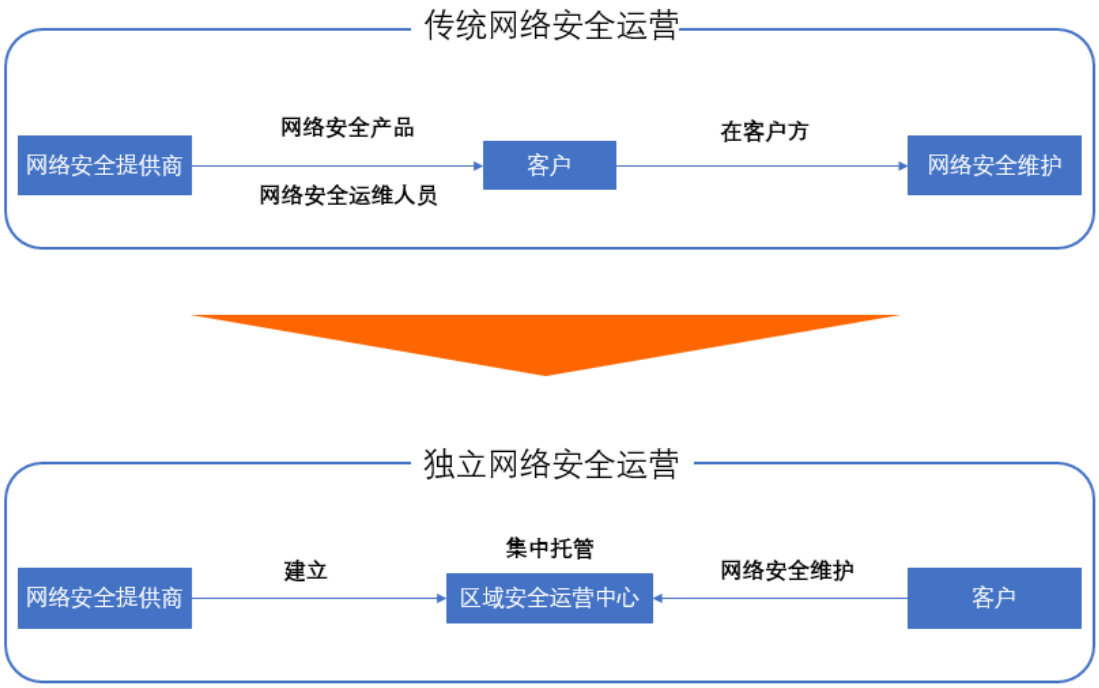
图 6 2012-2016 年我国网络安全事件数量及增长率



数据来源：国家互联网应急中心

随着国内信息安全事件频发，近些年各级政府和企事业单位在网络建设的过程中投入大量资金购买专业的信息安全产品和服务，但在实际操作过程中还存在一些不足，为最大发挥信息安全产品的价值，提升信息安全事件的防御能力，启明星辰建立区域安全运营中心，将政府和企事业单位的信息安全业务进行集中托管，为客户提供有效的整体安全服务，通过专业的安全运维人员和专家分析团队为客户提供 7*24 小时的安全监测和感知能力，并且在各个城市安全运营中心间建立横向沟通机制，在各个运营中心的系统层面建设威胁情报传递功能，建立安全事件的快速应急响应体系，从而有效提高应对信息安全事件的防御能力，保障政府机构和企事业单位的信息系统正常、持续运行。

图 7 网络安全运营行业发展趋势



（二）智慧城市的发展需要

2014 年国家发改委、工信部等 8 部委联合发布《促进智慧城市健康发展的指导意见》其中意见指出到 2020 年建设一批智慧城市，并且要求智慧城市发展实现网络安全长效化机制。使得国内智慧城市建设迅速走上快轨道，成为增强城市综合竞争力、打造区域经济发展新引擎、破解城市发展难题的新抓手。

我国住建部、发改委、工信部等重要部门均参与智慧城市试点规划，截至 2015 年共规划了 686 个试点，试点城市将经过 3-5 年的创建期，住建部将组织评估，对评估通过的试点城市(区、镇)进行评定，评定等级由低到高分为一星、二星和三星，

由此促进产业快速发展。

表格 1 中国智慧城市试点城市统计

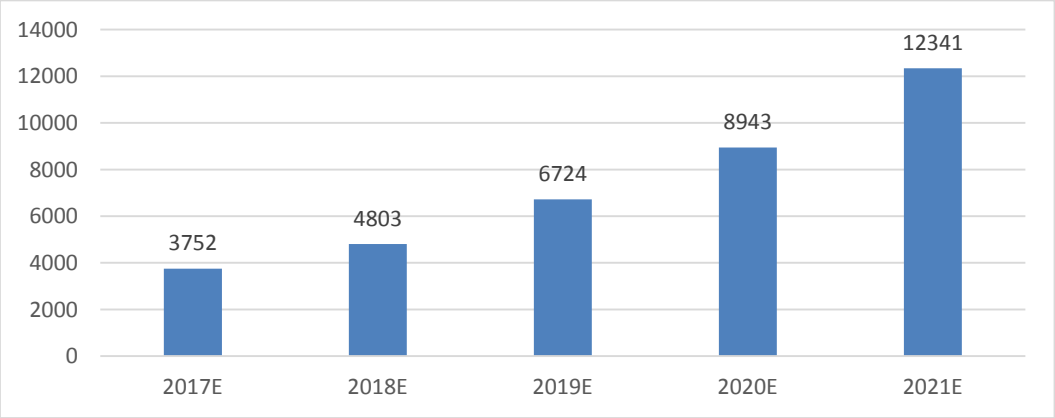
试点年份	部位名称	试点名称	试点数量
2012	住建部	国家智慧城市试点（第一批）	90
	科技部和国家标准委	智慧城市技术和标准试点	20
2013	住建部	国家智慧城市试点（第二批）	新增试点 103 个 扩大试点 9 个
	工信部	国家信息消费试点（第一批）	68
	国家测绘地理信息局	智慧城市时空信息云平台试点（第一批）	10
	工信部	基于云计算的电子政务公共平台试点示范	77
2014	住建部	国家智慧城市试点（第三批）	新增试点 84 个 扩大试点 13 个 专项试点 41 个
	工信部	国家信息消费试点（第二批）	36
	国家测绘地理信息局	智慧城市时空信息云平台试点（第二批）	10
	国家发改委	信息惠民国家试点城市	80
	工信部与国家发改委	宽带中国示范城市（城市群）	39
	国家发改委	宽带乡村试点工程（一期）	6
总计		**7 类试点**	**686 个试点**

数据来源：住建部、工信部、发改委、国家测绘地理信息局、科技部和国家标准委

智研咨询报告研究表明 2014 年，中国智慧城市 IT 投资规模达 2,060 亿元，较 2013 年同期增长 17.0%；2015 年，中国智慧城市 IT 投资规模达 2,480 亿元，较 2014 年同期增长 20.4%。预计 2017 年中国智慧城市 IT 投资规模将达到 3,752 亿元，未来五年（2017-2021）年均复合增长率约为 31.12%，2021 年 IT 投资规模将达到 12,341 亿元。

图 8 2017-2021 年中国智慧城市 IT 投资规模预测

单位：亿元



数据来源：智研咨询

尽管我国政府机构、行业企业、科研单位等实体组织做了大量行之有效的工作，但智慧城市在信息安全层面仍存在一些问题和风险，例如：

- **智慧城市数据安全风险**

智慧城市中存储了海量城市数据信息，涉及政务、医疗、社保、交通等行业，而智慧城市的核心之一便是不同行业之间多元数据的共享与融合。如何确保海量数据在融合与使用过程中居民个人隐私信息、企业和政府敏感数据不被入侵篡改和肆意泄露，有效保障智慧城市大数据安全，无疑是智慧城市建设过程中面临的艰巨任务。

- **物联网技术安全风险**

众所周知，绝大部分物联网设备在安全性上十分脆弱，甚至不具备任何自我保护能力：首先是无人值守的各类传感器很容易受到外界环境或人为的破坏影响而失去效用；其次是家用路由器、智能电视、智能冰箱等智能家居系统，以及智能监视器、医用联网设备、工业控制联网设备等甚至没有任何安全防护措施，极有可能因自身漏洞受到恶意攻击停止服务，或被利用发起分布式拒绝服务（DDoS）攻击；最后是物联网设备在通过无线网络传输信息时存在被干扰、截获或破解的安全威胁。

- **智慧城市关键技术存在失控风险**

智慧城市高度集成了物联网、云计算、大数据、移动互联网等众多新形态的信息通信技术，是一项复杂的大型系统集成工程。其中涉及到的芯片技术、通信技术、软件系统等关键技术我国科技界还没有完全掌握，其中隐藏着大量的潜在风险。这对于智慧城市运营管理而言，面临的安全风险和隐患之大不可想象。

区域安全运营中心的设立，可以近距离的为智慧城市发展提供安全保障，通过高效、专业的网络安全服务，让整个城市的运行更加安全、顺畅。所以，智慧城市的迅速发展为启明星辰区域安全运营中心的成功提供了良好的契机。

（三）公司战略发展的需要

建立区域安全运营中心和网络安全培训中心符合启明星辰的战略发展规划和布局。

近些年，启明星辰的业务模式不断创新，现阶段以及未来的发展重点在安全独立运营、安全技术的互联网+（针对云计算、物联网、大数据、移动互联等）和人工智能化的安全能力建设上。通过与启明星辰在全国各地的生态资源加强合作，

投入建设独立安全运营中心，并嵌入互联网+与 AI 的能力，为客户提供更优质的网络安全服务。

建立区域安全运营中心，将进一步扩大启明星辰在该省份的市场份额以及信息安全服务能力，能够快速抓住市场先机，完成战略上的布局，成为中国最具主导地位的企业级网络安全服务提供商。建立网络安全培训中心，不仅能够为企业提供更多专业的人才，还能够向社会供应人才，增强国家信息安全防护能力，从而提升启明星辰的品牌影响力。

（四）更好的满足地方政府和企业的需要

根据“谁主管，谁负责”的原则，同时鉴于数据的保密性要求与维护便利需求，当地政府和企业要求在其所辖区域内提供数据的存储、使用和服务，例如全国首部大数据地方法规《贵州省大数据发展应用促进条例》中规定“省人民政府建立数据安全工作领导协调机制，统筹协调和指导本省数据安全保障和监管工作”，“大数据采集、存储、清洗、开发、应用、交易、服务单位应当建立数据安全防护管理制度,制定数据安全应急预案,并定期开展安全评测、风险评估和应急演练；采取安全保护技术措施,防止数据丢失、毁损、泄露和篡改,确保数据安全。发生重大数据安全事故时,应当立即启动应急预案,及时采取补救措施,告知可能受到影响的用户,并按照规定向有关主管部门报告。”所以只有在辖区本地设立安全运营中心，才既能够满足客户对于信息安全的需求，也能够保障在遇到信息安全问题时，能够快速反应。

四、本次募集资金投资项目实施的可行性

（一）该项目具有良好的市场前景

1、信息安全市场行业痛点多，市场潜力巨大

由于各行业对网络系统的依赖越来越强，攻击造成的业务停止服务的危害、以及公民个人信息为代表的数据泄露、损毁所造成的影响越来越大，甚至在某些情况下，安全事件会直接导致公民生命安全受到威胁；但是深入的分析，现有的安全解决方案还是基于传统的产品部署模式和服务模式，不足以面对不断升级的网络安全攻击行为。

2017 年 5 月，当我们应对 WannaCry 勒索病毒的威胁时所采用的方法，与十余年前应对冲击波、震荡波蠕虫病毒时的手段并未有本质的区别，还是依靠断网、

单机查杀病毒去处理，从造成这种现象的原因分析看，主要在以下几个方面：

➢ **在网络运营者一侧的问题：**

各类机构在网络建设的过程中采购了大量安全产品，但是缺乏专业使用人员，导致无法确认安全产品是否在正常发挥作用；安全产品的无效部署带来虚假的安全感，可能会因为问题处理不及时，反而造成的损失会更高。

➢ **在安全设备厂商一侧的问题：**

安全厂商在新技术领域不断研究推出新型产品，如最近结合威胁情报、大数据分析推出的相关态势感知类、高级威胁防御类产品，但是此类产品对于前端使用人员的要求不是降低，而是更高；产品距离用户需求非但没有拉近，而是更远。

➢ **传统网络安全服务的局限：**

传统的安全服务是安全评估、渗透测试、安全咨询类服务，此类服务都是基于年度或单次的安全服务，只能在某个阶段对某一特定系统的安全状态进行评价，无法持续的进行监测以应对持续的来自内外部的威胁。

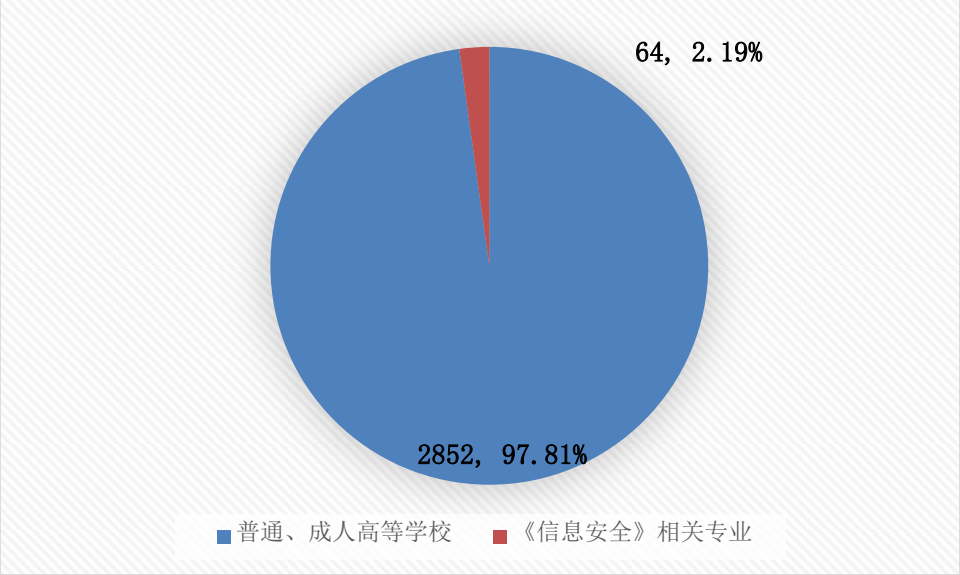
所以，区域安全运营中心可以利用云计算、大数据等先进技术为当地的客户提供高效的网络安全运营和维护服务，可以有效缓解政府、企业网络安全运营人员短缺和能力不足的问题，通过集中、持续的网络安全监测，提高政府、企业面对网络安全突发事件的应急能力，减少损失，从而有效缓解长期困扰客户网络安全运营的难题。

2、中国网络安全人才供应严重不足

（1）中国网络安全人才匮乏

根据智联招聘发布的 2017 年的《网络安全人才市场状况研究报告》的数据显示，2017 年上半年，通过智联招聘发布的网络安全岗位招聘需求，较 2016 年上半年同比增长了 232%。但根据教育部 2015 年发表的《中国教育概况》的数据显示，2015 年，全国共有普通、成人高等学校 2,852 所，但开设《信息安全》相关专业的院校仅有 64 所，占比仅为全国高等学校总数的 2.2%。信息安全专业的学生培养滞后于市场的需求。

图 9 2015 年开设《信息安全》相关专业的院校占比



数据来源：《中国教育概况--2015 年全国教育事业发展情况》

随着互联网技术的应用进一步普及，加上《网络安全法》、国家网络安全等级保护制度的强力推动，国内广大政企机构将会迅速形成对网络安全人才的紧迫需求。东南大学网络空间安全学院常务副院长程光在接受澎湃新闻采访时称，根据我国医生、护士对应全国总人口的比例来计算，我国信息安全人才缺口是 70 万；而以我国警民比例作为参考的话，计算出的结果大概在 70-140 万之间。

整个信息安全市场面临巨大的人才缺口，如果不能够增加人才供给量，未来信息安全人才缺口将越来越大。

（2）信息安全市场专业安全分析人才匮乏

目前，安全行业内人才培养偏重两类。第一类是大专院校培养的科班出身的安全人才，偏重于各类安全理论知识，缺乏应用经验；第二类是各类攻防演练平台培养的安全人才，偏重于攻击渗透，但缺乏安全事件分析、防御方面的体系化能力。专业的安全分析师十分稀缺，且集中在专业的信息安全公司，一些政府机构和其他领域企业难以获得这方面的人才。

整个信息安全市场面临巨大的人才缺口，如果不能够增加人才供给量，未来信息安全人才缺口将越来越大。网络安全培训中心的建立，可以不断地为国家培养信息安全人才，满足市场需求。

（二）国家相关政策的大力支持

近几年，国家出台了大量的法律、法规，旨在推动信息安全市场的健康有序发展，为独立安全运营中心的建立，提供了政策支持。

表格 2 信息安全相关政策

时间	发文单位	名称	主要内容
2016 年	全国人大常委会	《网络安全法》	进一步界定关键信息基础设施范围；对攻击、破坏我国关键信息基础设施的境外组织和个人规定相应的惩治措施；增加惩治网络诈骗等新型网络违法犯罪活动的规定等
2015 年	工信部	《国务院关于积极推进“互联网+”行动的指导意见》	加快安全可靠服务器、存储系统、桌面计算机及外部设备、网络设备、智能终端等终端产品、基础软件和信息系统的研发与推广
2014 年	工信部	《加强电信和互联网行业网络安全工作的指导意见》	对网络基础设施和业务系统安全防护、推进安全可控关键软硬件应用、网络数据和用户个人信息保护等做出强调。
2014 年	中央军委	《关于进一步加强军队信息安全工作的意见》	加强信息安全工作是适应信息时代发展的必然要求，是实现能打仗打胜仗核心要求的紧迫任务，必须把信息安全工作作为军事斗争准备的保底工程，采取超常、务实举措解决突出矛盾和重难点问题，促进我军信息化建设科学发展、安全发展。
2014 年	银监会	《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》	从 2015 年起，各银行业金融机构对安全可控信息技术的应用以不低于 15%的比例逐年增加，并要求安排不低于 5%的年度信息化预算，到 2019 年安全可控信息技术在银行业总体达到 75%左右的使用率。

资料来源：整理于公开资料

（三）启明星辰是国内信息安全领域的领军企业

1、产品线充裕完备，多领域位居首位

公司成立于 1996 年，是国内少数拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。

在产品方面，公司拥有完善的专业安全产品线，横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域，共有百余个产品型号，并根据客户需求不断增加。其中统一威胁管理（UTM）、入侵检测与防御（IDS/IPS）、安全管理平台（SOC）均取得市场占有率第一的成绩（赛迪报告 2015,2016），同时在安全性审计、安全专业服务方面保持市场领先地位，其它还包括防火墙（FW）、Web 应用防火墙、漏洞扫描、互联网行为管控、终端安全、数据防泄密、无线安

全引擎、应用交付、网闸、数据安全交换、大数据处理/安全、电子印章/签名、工控安全等多个产品类型。随着云计算时代的到来，公司已完成大部分产品的虚拟化、云化工作，并推出满足政务云/行业云、大数据应用、智慧城市、态势感知、移动互联安全等新需求的新产品与解决方案。

表格 3 启明星辰主要产品

产品类别	说明
安全网关	部署于网络边界、出口的安防产品，主要包括防火墙、NGFW、UTM、VPN 网关、网闸、抗 DDoS 等
安全检测	部署于网络内部中深层的安防产品，主要包括 IDS/IPS、网络审计、内网安全管理等；
数据安全与平台	以数据为基础或对象的安管产品，主要包括 SOC、4A、DLP、数据交换、大数据处理分析等
安全服务与工具	包括风险评估、监控应急、安全运维、系统支持等服务以及相关工具类产品
硬件及其他	为用户提供安全解决方案、系统集成项目而用到的第三方硬件等。

资料来源：启明星辰 2017 年年报

2、公司在行业中具有技术服务优势

在安全攻防技术领域，公司已经达到国际先进水平，拥有多年积累的丰富的攻防技术核心知识库，IDS/IPS 攻击特征库、漏洞库、蠕虫机理、审计的行业规则库等已经成为公司的核心技术能力，有力支持了公司各相关产品的研发，并为公司持续保持技术优势以及今后的发展打下坚实基础。

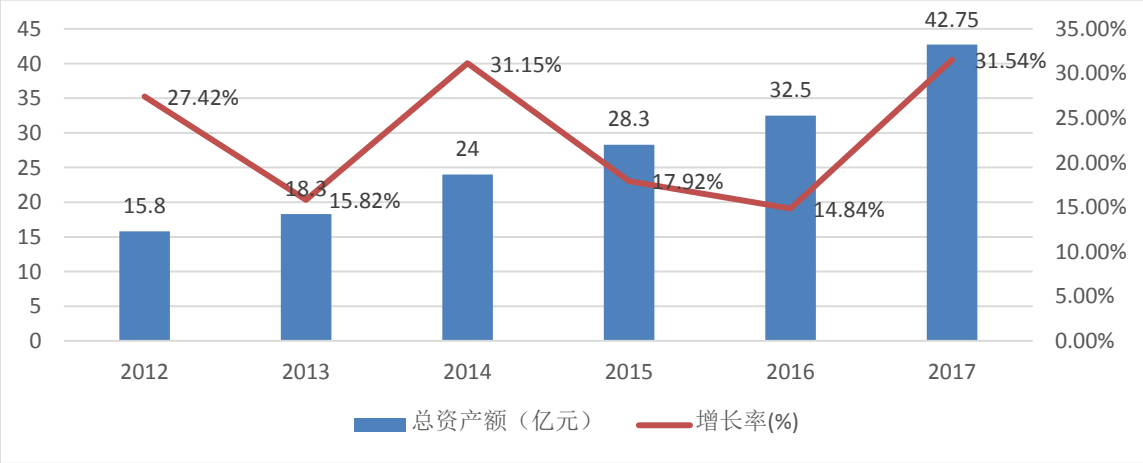
雄厚的技术实力使得公司成为国内信息安全领域国家级重点科研项目的主要承担者之一，拥有国家级网络安全技术研发基地，获得百余项自主知识产权，填补了国家多项空白，处于业界领先地位。

秉承最佳实践的理念，在启明星辰 TSP（诚信的安全产品、安全服务、安全解决方案提供商）理念的指导下，在公司系列安全产品大规模部署和使用的基础上，多年来启明星辰已经承担了千余项大中型信息安全风险评估、安全管理与监控、安全管理咨询、应用系统安全性分析、安全运维等方面的安全服务工程，以及近百项重点国家项目。结合国际先进的安全事件预警与响应经验，经过在政府、电信、金融、能源、军队、交通、传媒、教育、军工等数百家重点行业客户单位的长时间实践，启明星辰已经形成一套全面、细致的专业安全服务体系，并成为国内有实力的安全服务提供商。

3、公司的良好盈利能力为战略性扩张打下基础

自成立以来，启明星辰销售业绩已连续多年保持高速增长。年度财务审计报告显示，截止到 2017 年 12 月 31 日，公司及其权益核算的合资公司总资产 42.75 亿元，净资产 31.77 亿元。近三年来，总资产保持稳定的增长态势。

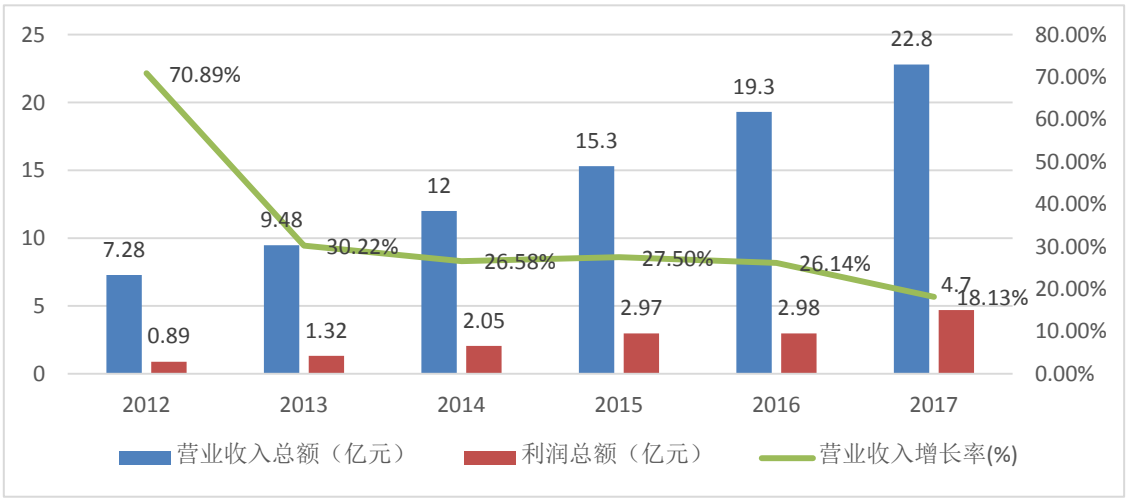
图 10 2012-2017 年启明星辰资产总额与增长率



数据来源：启明星辰年度审计报告

2017 年，启明星辰实现营业总收入 22.8 亿元，利润总额 4.70 亿元。近五年来，营业收入保持持续增长，增长率都保持在 18%以上，利润也呈增长趋势，复合增长率为 31.96%，公司财务状况良好。

图 11 2012-2017 年启明星辰营业收入总额、利润及增长率



数据来源：启明星辰年度审计报告

显而易见，启明星辰的良好盈利能力为战略性扩展打下基础。

五、本次募集资金投资项目的具体情况

（一）济南安全运营中心建设项目

1、项目概述

项目名称为济南安全运营中心建设项目，由公司的全资子公司负责实施，项目总投资为 9,200 万元，拟投入本次公开发行可转债募集资金 5,700 万元，自筹资金 3,500 万元。本项目通过购买办公楼、配置先进的硬件设备和软件工具，整合启明星辰生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为山东省的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力；从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

2、项目必要性分析

在济南建立区域安全运营中心符合启明星辰的战略发展规划和布局。建立济南安全运营中心，将进一步扩大启明星辰在山东省的市场份额以及服务能力，能够快速的抓住市场先机，完成战略上的布局，成为中国最具主导地位的企业级网络安全服务提供商。因此，本项目的实施非常有必要。

3、项目可行性分析

公司在山东拥有良好的品牌基础，济南拥有完整的核心技术团队，团队在山东省内的传统产品与安全服务领域具有 10 余年的历史积累，营造了非常高的品牌认同度，且培育了一大批认同前沿技术方向的客户群体，可以快速的开展安全运营业务，形成盈利，同时也可以为安全运营业务内容提供最佳实践经验。因此，本项目实施可行。

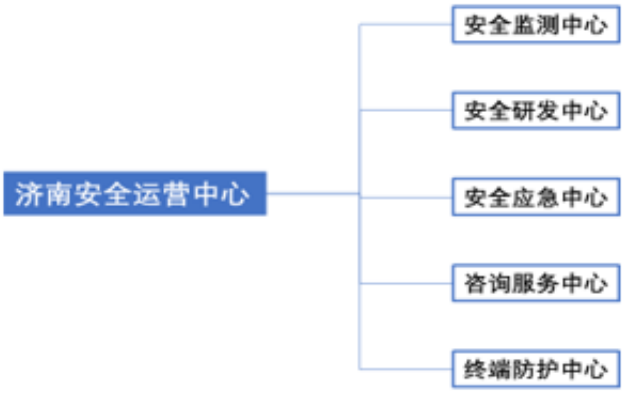
4、项目的建设主要内容

济南安全运营中心通过整合启明星辰生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力；从而能够满足对各类网络安全行

为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

主要包括：安全检测中心、安全应急中心、安全研究中心、咨询服务中心、终端防护中心。

图 12 济南安全运营中心建设内容



资料来源：启明星辰内部资料

基于云端数据与分析中心汇聚的安全大数据，整个核心分析团队会开展更为广泛与深入的安全研究，实现公司在安全技术各个领域内的研究能力与安全数据之间的有机结合。

5、项目投资概况

投资总额为 9,200 万元，其中建设投资 5,700 万元，研发费用：2,500 万，铺底资金 1,000 万元，将主要用于济南运营中心楼房购买、装修，研发设备购买，研发费用和铺底资金等。具体资金运用情况见下表：

表格 4 济南安全运营中心项目投资估算表

单位：万元

	购置办公场所	装修	设备	研发费用	铺底资金	合计
投资额	3,574	273	1,853	2,500	1,000	9,200
各项比例占总投资	38.85%	2.97%	20.14%	27.17%	10.87%	100%

6、项目财务评价

本项目建设期为 2.5 年，第 3 年进入经营期。本项目全部达产后预计年均销售收入为 5,774.85 万元，年均净利润 2,122.17 万元，扣除所得税后内部收益率 22.22%，静态投资回收期（税后，含建设期）为 5.93 年。从产品的市场及项目经济效益等方面分析来看，本项目具有较好的市场前景和财务经济效益。

（二）杭州安全运营中心建设项目

1、项目概述

项目名称为杭州安全运营中心建设项目，由公司的全资子公司负责实施，项目总投资为 28,000 万元，拟投入本次公开发行可转债募集资金 13,500 万元，自筹资金 14,500 万元。本项目通过购买办公楼、配置先进的硬件设备和软件工具，整合启明星辰生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力；从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

2、项目必要性分析

在杭州建立安全运营中心符合启明星辰的战略发展规划和布局。建立杭州安全运营中心，将进一步扩大启明星辰在浙江省的市场份额以及服务能力，能够快速的抓住市场先机，完成战略上的布局，成为中国最具主导地位的企业级网络安全服务提供商。因此，本项目的实施非常有必要。

3、项目可行性分析

在建设移动智慧城市方面，浙江省一直走在全国前列，为杭州区域安全运营中心营造了良好的市场环境。杭州市作为浙江省的省会，围绕着自主创新、网络安全和中国智造，打造了网络信息技术产业的完整产业链，形成了千亿级信息经济（智慧经济）产业，具备了可以代表国家参与全球竞争的优势，涌现了阿里巴巴、华三通信、海康威视、浙江中控、聚光科技等一大批行业领军企业，形成了电子商务、智慧互联、智慧物联、智慧医疗、智慧安防、智慧环保等“互联网+”的产业集群，电子商务、数字视频监控、宽带接入设备、集成电路设计产业、软件产业、动漫制作的整体水平居国内领先。2016 年高新技术产业营业收入超 4,200 亿元，其中网络信息技术产业收入 2,253 亿元，增长 20%。因此，本项目实施可行。

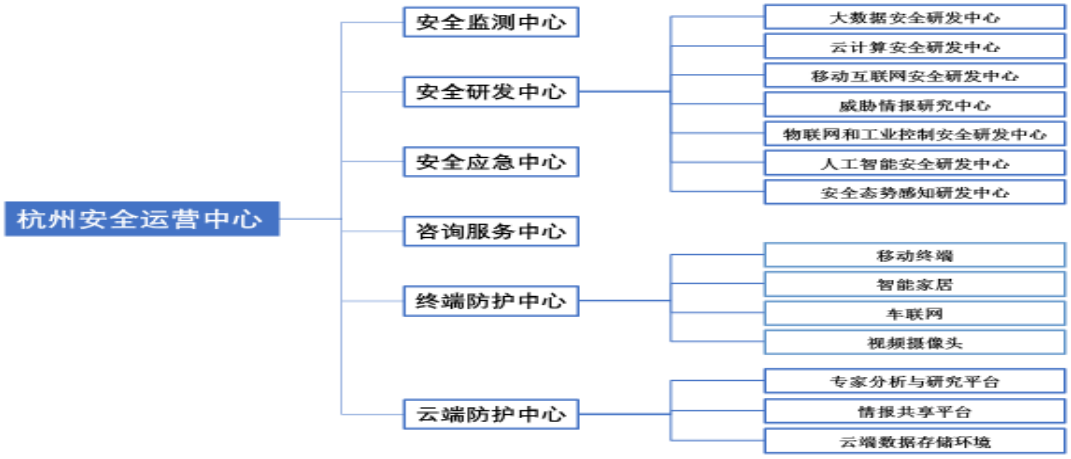
4、项目的建设主要内容

杭州安全运营中心通过整合启明星辰生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中

心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力；从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

主要包括：安全检测中心、安全应急中心、安全研究中心、咨询服务中心、终端防护中心和云端防护中心，并在研发中心的基础上建立大数据安全研究中心、云计算安全研究中心、移动互联网安全研究中心、威胁情报研究中心、物联网和工业控制安全研发中心、人工智能安全研究中心、安全态势感知研发中心等多个前沿性安全研究和开发子中心；终端防护中心包括移动终端、智能家居、车联网、视频摄像头；云端防护中心包括专家分析与研究平台、情报共享平台、云端数据存储环境。

图 13 杭州安全运营中心建设内容



资料来源：启明星辰内部资料

基于云端数据与分析中心汇聚的安全大数据，整个核心分析团队会开展更为广泛与深入的安全研究，实现公司在安全技术各个领域内的研究能力与安全数据之间的有机结合。

5、项目投资概况

本项目投资总额为 28,000 万元，其中建设投资 13,500 万元，研发费 12,000 万，铺底资金 2,500 万元，将主要用于杭州运营中心楼房购买、装修，研发设备购买，研发费用和铺底资金等。具体资金运用情况见下表：

表格 5 杭州安全运营中心项目投资估算表

单位：万元

	购置办公场所	装修	设备	研发费用	铺底资金	合计

投资额	8,000	2,000	3,500	12,000	2,500	28,000
各项比例占总投资	28.57%	7.14%	12.50%	42.86%	8.93%	100%

6、项目财务评价

本项目建设期为 2.5 年，第 3 年进入经营期。本项目全部达产后预计年均销售收入为 17,294 万元，年均净利润 6,282.98 万元，扣除所得税后内部收益率 20.74%，静态投资回收期（税后，含建设期）为 6.14 年。从产品的市场及项目经济效益等方面分析来看，本项目具有较好的市场前景和财务经济效益。

（三）昆明安全运营中心和网络安全培训中心建设项目

1、项目概述

项目名称为昆明安全运营中心和网络安全培训中心建设项目，由公司在昆明的全资子公司负责实施，项目总投资为 47,300 万元，拟投入本次公开发行可转债募集资金 37,300 万元，自筹资金 10,000 万元。本项目通过建造办公楼、配置先进的硬件设备和软件工具，整合启明星辰生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力，从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

2、项目必要性分析

在昆明建立区域安全运营中心符合启明星辰的战略发展规划和布局。建立昆明安全运营中心，将进一步扩大启明星辰在云南省的市场份额以及服务能力，能够快速的抓住市场先机，完成战略上的布局，成为中国最具主导地位的企业级网络安全服务提供商。

国内网络安全形势严峻，政府及企事业单位的信息屡遭攻击，由于缺乏专业的网络安全运维人员，网络安全产品使用效率偏低，昆明网络安全培训中心的建立可以有效解决专业人员不足的难题，提高安全产品使用效率，并为国内外培养专业的网络安全人才。因此，本项目的实施非常有必要。

3、项目可行性分析

2017 年 5 月 27 日，启明星辰与云南省人民政府签署战略合作框架协议，与昆明市签署了落地项目合作协议。此次合作主动服务和融入国家“一带一路”发展战略，推动云南省“云上云”行动计划及各州市智慧城市和关键信息基础设施的积极防御和有效处置。合作涵盖多领域，覆盖全方位，从业务层面到科研层面均达成重大合作。根据协议，双方将在金融、能源、电力、通信、交通等领域开展网络安全防护合作，建立长期稳定的战略合作。启明星辰将在技术、资金、人才、团队等方面提供支持。同时，启明星辰将在云南成立“启明星辰区域总部”，整合网络安全相关资源，引领网络安全行业健康发展。云南省将全力支持启明星辰建设“启明星辰网络安全培训中心”，为西南区域和南亚东南亚国家网络空间安全后续的研究和建设提供科学研究和人才培养。

同时，信息产业园高校片区驻有云南大学、昆明理工大学等九所重点高校，各类研究室、实验室为产学研究对接和一体化发展提供多重选择，近 18 万在校大学生为校企合作提供充足资源。因此，本项目实施可行。

4、项目的建设主要内容

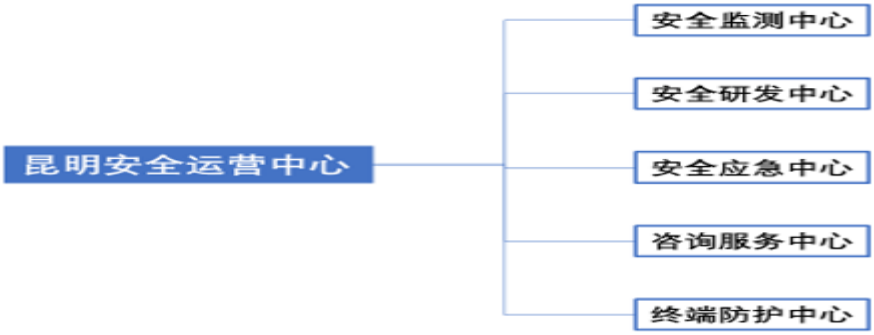
本项目的建设包括区域独立安全运营中心和网络安全培训中心两个部分组成。

（1）区域安全运营中心建设目标和主要内容

昆明安全运营中心通过整合启明星辰生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力；从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

昆明安全运营中心包括包括安全监测中心、安全应急中心、安全研发中心、咨询服务中心和终端防护中心。

图 14 昆明安全运营中心项目建设内容



资料来源：启明星辰内部资料

（2）网络安全培训中心建设目标和主要内容

昆明网络安全培训中心的目标是建设一流的网络安全培训中心，为国内外提供专业的网络安全人才。

昆明网络安全培训中心为组织客户（城市级客户、关键信息基础设施、大型政企客户、行业机构、中小企业、组织）和个人客户（在校大学生、应届毕业生、IT 从业想转型做安全的人员）提供网络安全培训服务，培训内容包括攻防渗透及竞赛培训、安全知识及前沿技术培训、国际国内安全认证培训，并为客户提供安全实验室建设方案、承办网络安全竞赛、安全人才培养方案咨询和定制化服务。

5、项目投资概况

投资总额为 47,300 万元，其中建设投资 37,300 万元，研发费用：6,000 万，铺底资金 4,000 万元，将主要用于昆明安全运营中心和网络安全培训中心的楼房购买、装修，研发设备购买，研发费用和铺底资金等。具体资金运用情况见下表：

表格 6 昆明安全运营中心和网络培训中心项目投资估算表

单位：万元

	土地购置款	基建	装修	设备	研发费用	铺底资金	合计
投资额	1,800	22,000	7,500	6,000	6,000	4,000	47,300
各项比例占总投资	3.81%	46.51%	15.86%	12.68%	12.68%	8.46%	100%

6、项目财务评价

本项目建设期为 3 年，第 4 年进入经营期。本项目全部达产后预计年均销售收入为 34,619.58 万元，年均净利润 13,241.99 万元，扣除所得税后内部收益率 20.78%，静态投资回收期（税后，含建设期）为 6.33 年。从产品的市场及项目经济效益等方面分析来看，本项目具有较好的市场前景和财务经济效益。

（四）郑州安全运营中心和网络培训中心建设项目

1、项目概述

项目名称为郑州安全运营中心建设项目，由公司的全资子公司负责实施，项目总投资为 50,500 万元，拟投入本次公开发行可转债募集资金 37,500 万元，自筹资金 13,000 万元。本项目通过购买办公楼、配置先进的硬件设备和软件工具，整合启明星辰生态圈内的各项优势技术资源，建立 7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力；从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

2、项目必要性分析

在郑州建立区域安全运营中心符合启明星辰的战略发展规划和布局。建立郑州安全运营中心，将进一步扩大启明星辰在河南省的市场份额以及服务能力，能够快速的抓住市场先机，完成战略上的布局，成为中国最具主导地位的企业级网络安全服务提供商。

国内网络安全形势严峻，政府及企事业单位的信息屡遭攻击，由于缺乏专业的网络安全运维人员，网络安全产品使用效率偏低，郑州网络安全培训中心的建立可以有效解决专业人员不足的难题，提高安全产品使用效率，并为国内外培养专业的网络安全人才。因此，本项目的实施非常有必要。

3、项目可行性分析

启明星辰在网络安全行业深耕二十多年，有丰富的安全技术积累、网络安全产品线和网络安全培训经验，拥有国内一流的网络安全产品研发团队，除此之外国家出台一系列政策鼓励推动该行业向好发展。

区内设有多个高校和各类研发机构，如解放军信息工程大学、郑州大学、河南工业大学、郑州轻工业学院等省内最知名的高校，为网络安全培训中心提供了大量的客户。因此，本项目实施可行。

4、项目的建设主要内容

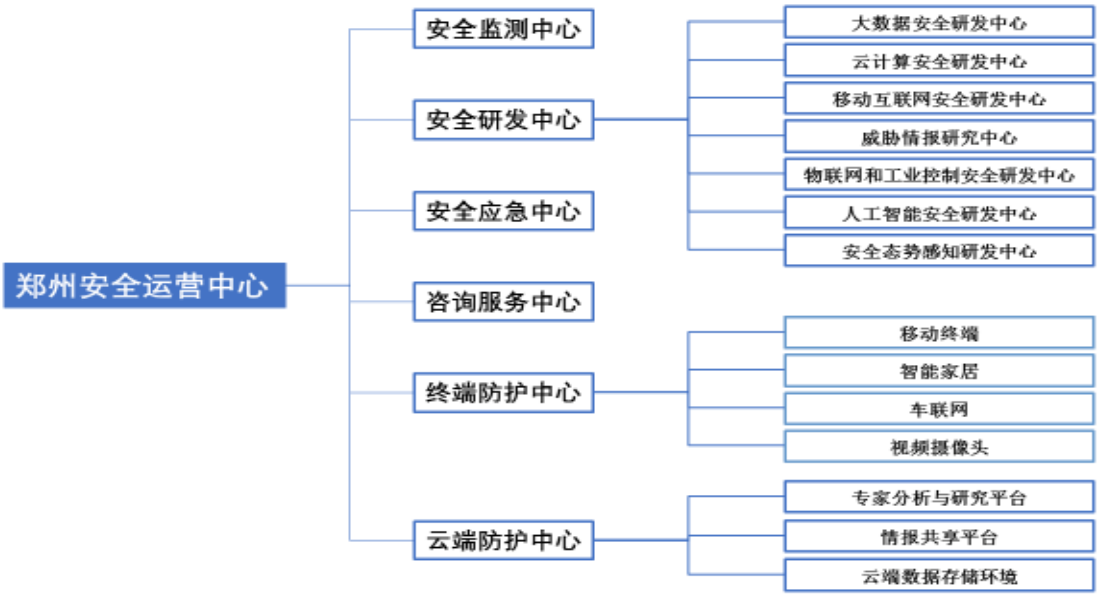
本项目的建设包括郑州安全运营中心和网络安全培训中心两个部分组成。

（1）郑州安全运营中心建设目标和主要内容

郑州安全运营中心通过整合启明星辰生态圈内的各项优势技术资源，建立7*24 小时的信息安全监控运营机制，为区域城市的智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知能力，从而能够满足对各类网络安全行为的监测要求，实现重大网络安全事件响应和处理能力，以应对不断变化的网络威胁形势，为区域经济和社会发展提供有效的网络安全保障能力。

主要包括：安全检测中心、安全应急中心、安全研究中心、咨询服务中心、终端防护中心和云端防护中心，并在研发中心的基础上建立大数据安全研究中心、云计算安全研究中心、移动互联网安全研究中心、威胁情报研究中心、物联网和工业控制安全研发中心、人工智能安全研究中心、安全态势感知研发中心等多个前沿性安全研究和开发子中心；终端防护中心包括移动终端、智能家居、车联网、视频摄像头；云端防护中心包括专家分析与研究平台、情报共享平台、云端数据存储环境。

图 15 郑州安全运营中心项目建设内容



资料来源：启明星辰内部资料

（2）网络安全培训中心建设目标和主要内容

郑州网络安全培训中心的目标是建设一流的网络安全培训中心，为国内外提供专业的网络安全人才。

郑州网络安全培训中心为组织客户（城市级客户、关键信息基础设施、大型政企客户、行业机构、中小企业、组织）和个人客户（在校大学生、应届毕业生、IT 从业想转型做安全的人员）提供网络安全培训服务，培训内容包括攻防渗透及竞赛培训、安全知识及前沿技术培训、国际国内安全认证培训，并为客户提供安全实验室建设方案、承办网络安全竞赛、安全人才培养方案咨询和定制化服务。

5、项目投资概况

投资总额为 50,500 万元，其中建设投资 37,500 万元，研发费用 10,000 万，铺底资金 3,000 万元，将主要用于郑州安全运营中心和网络安全培训中心的楼房购买、装修，研发设备购买，研发费用和铺底资金等。具体资金运用情况见下表：

表格 7 郑州安全运营中心项目投资估算表

单位：万元

	购置办公场所	装修	设备	研发费用	铺底资金	合计
投资额	24,000	7,500	6,000	10,000	3,000	50,500
占总投资的比例	47.52%	14.85%	11.88%	19.80%	5.95%	100%

6、项目财务评价

本项目建设期为 3 年，第 4 年进入经营期。本项目全部达产后预计年均销售收入为 38,325.95 万元，年均净利润 14,659.68 万元，扣除所得税后内部收益率 20.36%，静态投资回收期（税后，含建设期）为 6.38 年。从产品的市场及项目经济效益等方面分析来看，本项目具有较好的市场前景和财务经济效益。

（五）补充流动资金

1、项目基本情况

公司拟使用本次募集资金 15,000.00 万元用于补充公司流动资金，增强公司的资金实力，促进公司业务实力的提升，支持公司长远战略发展。

2、项目的必要性

本次补充流动资金，将有利于支持公司的长远发展战略的实施：

首先，报告期内，公司信息安全业务增长迅速，营业收入年增长率平均保持在 25%以上，公司产品线不断扩充，新产品市场积极开拓，公司业务运营对资金需求不断增加，本项目将有效缓解公司营运资金压力，增强公司资金实力；

其次，公司作为国内信息安全领域的龙头企业，需要持续关注信息安全技术领域的最新科研成果，通过加大高端人才培养与引进力度，拓展产学研合作范围，

维持公司的核心技术优势，公司未来需要保持较高的研发投入，本项目的实施将有效推动公司研发活动的开展；

最后，公司通过使用部分募集资金补充流动资金，可以使公司的资金结构更加合理，提高公司的资金使用效率，从而提高公司的经营效率。

综上所述，公司拟使用部分募集资金补充流动资金，有利于支持公司的长远发展战略的实施，增强公司的资金实力，推进公司研发活动，提高公司的经营效率。因此，本项目实施具有必要性。

六、本次发行对公司经营管理、财务状况的影响

（一）本次发行对公司财务状况的影响

本次募集资金投资项目符合国家产业政符、行业发展趋势以及公司的发展战略，具有良好的市场发展前景和经济效益，随着相关项目效益的逐步实现，公司的盈利能力将得到进一步的提升。

本次发行完成后，公司的资产规模将进一步扩大，募集资金到位后，公司的流动资金将更加充裕，有利于增强公司的资本实力。如本次可转换公司债券发行完成并逐渐转股后，公司资产负债率将会逐步降低。

（二）本次发行对公司经营情况的影响

本次募投项目的建设有利于公司提高对政府机构、企业及网络空间危害事件的发现与响应能力、加强潜在攻击的监测和调查能力，使公司的业务结构、技术水平、市场开拓水平等得到显著提高；同时补充流动资金有助于公司减少资金压力，扩大业务规模，加大研发投入。

因此，本次发行有利于提高公司的核心竞争能力，进一步提升公司的盈利能力、行业地位。

启明星辰信息技术集团股份有限公司董事会

2018 年 4 月 14 日