东兴证券 DONGXING SECURITIES

密码资质构筑强力护城河，打造党政军综合信息安全服务商

——卫士通（002268）深度报告

2018 年 08 月 21 日

强烈推荐/首次

卫士通 | 深度报告

陆洲

010-66554142 luzhou@dxzq.net.cn

执业证书编号: S1480517080001

王习

010-66554034 Wangxi@dxzq.net.cn

执业证书编号: S1480518010001

研究助理：张高艳

021-25102859 Zhanggy_yjs@dxzq.net.cn

执业证书编号: S1480116080036

研究助理：张卓琦

010-66554018 Zhangzq_yjs@dxzq.net.cn

执业证书编号: S1480117080010

报告摘要：

密码业务是公司最重要的护城河。信息安全分为两类：一类是网络安全，本质是隔离，防止信息跑出去。该业务发展逻辑是动态的攻防过程，需要不停的技术迭代，是一个 know-how 的过程。此类厂商是启明星辰，深信服，360 等；另一类是信息被加密，即使泄露也无法读取，这类就是密码学，由国家指定的，最核心的竞争力是资质。而卫士通恰恰是具备这一资质的，是上市公司中唯一的信息安全国家队。

公司有望转型党政军网络信息安全服务商。公司从安全产品提供商到安全服务整体解决方案提供商，改变了原来“产品交付”模式；也解决了企业对网络本身安全防护手段较多，但对数据安全保护较少的困境，提升整体防护水平。此外，此次华丽转身也将提升卫士通的盈利水平，从原来的交付产品模式转变为每年收取交运营管理费的模式，令收入曲线更加平滑，其对下游的话语权也将提升，有效提高毛利率水平。随着传统优质央企需求的转变，公司有望迎来新一轮增长。

与阿里云合作卡位安全云，奠定在党政军自主可控安全云平台生态链中的优势地位。公司具备信息安全国家队资质优势以及在央企中网络安全先进的运维经验，有望结合阿里云的技术优势，在未来党政军自主可控安全云平台中取得更大市场份额。历史上来看，公司于 2014 年安全集成服务从 1.65 亿跃升为 6.96 亿，此次与阿里云强强联合，有望在安全集成领域掀起另一轮高增长态势。党政军上云规模预计不低于 5000 朵云，如果安全服务按照 300 万的价格，其市场规模将达到 150 亿，助力公司新一轮业绩飞跃。

公司有望成为 5G 军用通信运营商，成功卡位未来网络战主力地位。5G 通信会引入多无线接入、SDN、云计算、NFV 等技术，这些技术使得网络边界变得十分模糊，以前依赖物理边界防护的安全机制难以得到应用，安全机制要适应虚拟化、云化的需要。卫士通提前卡位 5G 安全技术，成立了 5G 安全专项推进组，重点开展 5G 密码应用等研发。公司确立了以密码为基础的统一信任体系，构建多元分立的数据防护模型，建立整体性的安全服务基础设施，形成面向垂直行业的 5G 安全解决方案。

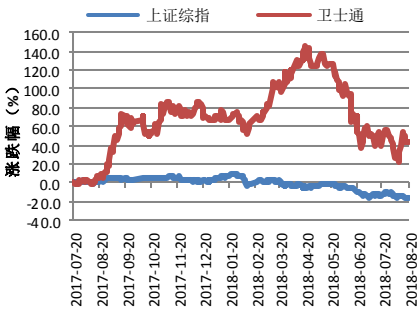
军队信息化中未来云计算应用不断深化，安全防护将成为核心问题。新军事变革要求建设战略云、作战云等基础设施，其面临的信息化打击包括：瘫痪云基础设施、通讯端泄密、数据链乃至数据库遭到袭击、电子干扰等。任何一种打击成功，对军队的安全都将是致命的。公司以信息加密起家，母公司中国网安目前在量子加密方面走在世界前列，在数据加密方面将有力保障军队信息安全；公司所在的中电科集团中在电子干扰方面具备多年深厚背景，具备雄厚的技术积累，与卫士通共同打造军用综合信息安全体系。

我们预计公司 2018 年、2019 年和 2020 年，收入分别为 30.14 亿元、52.27 亿元和 76.92 亿元，归母净利润分别为 2.45 亿元、5.47 亿元和 8.08 亿元，EPS 分别为 0.29 元、0.65 元和 0.96 元，首次覆盖给与给予公司“强烈推荐”

交易数据

52 周股价区间（元）	16.73- 34.72
总市值（亿元）	173
流通市值（亿元）	167
总股本/流通股（非限售）（百万股）	809.90/838.34
流通 B 股/H 股（万股）	

52 周股价走势图



资料来源：东兴证券研究所

相关研究报告

1、《国防军工行业点评报告：美国制裁，长期看显著利好电科研究所》2018-08-02

2、《国防军工行业 2018 年中期策略报告：严寒已过，春天在路上》2018-07-12

3、《国防军工行业报告：中电科核心研究所深度分析---中国电子科技集团公司专题报告》2018-05-02

4、《国防军工行业事件点评：建议关注“电科系”加速整合研究所》2017-11-17

评级。

风险提示：安全运维推广不达预期，政务云竞争激烈，5G 应用进度低于预期。

财务指标预测

指标	2016A	2017A	2018E	2019E	2020E
营业收入（百万元）	1,798.90	2,137.11	3,014.53	5,227.44	7,692.93
增长率（%）	12.2%	18.8%	41.1%	73.4%	47.2%
净利润（百万元）	155.75	150.30	245.01	547.78	807.90
增长率（%）	4.7%	-3.5%	63.0%	123.6%	47.5%
净资产收益率（%）	10.5%	3.5%	5.4%	10.8%	13.7%
每股收益(元)	0.19	0.18	0.29	0.65	0.96
PE	105.39	109.21	67.00	29.97	20.32
PB	11.02	3.82	3.61	3.23	2.78

资料来源：公司财报、东兴证券研究所

目录

表格目录

插图目录

1. 从网络安全产品商迭代为党政军网络信息安全服务商

2018 年 5 月 4 日，中国网络安全与信息产业峰会在成都召开。中国电子科技网络信息安全有限公司董事长李成刚在会上表示，欧美发达国家探索形成了“信息寡头+网络安全巨头+网络安全专业厂商群体+军工骨干企业”的四层产业格局，企业在国家网络安全保障中发挥了主力军作用，它们掌握着核心技术，占据产业价值链高端。在这点上，我国的网络安全产业发展是不足的。

不过，以卫士通为代表的企业有希望扛起保障国家网络安全的大旗。目前来看，卫士通在以下几方面的布局使其成为网络信息安全服务的翘楚：

1）密码技术自主可控

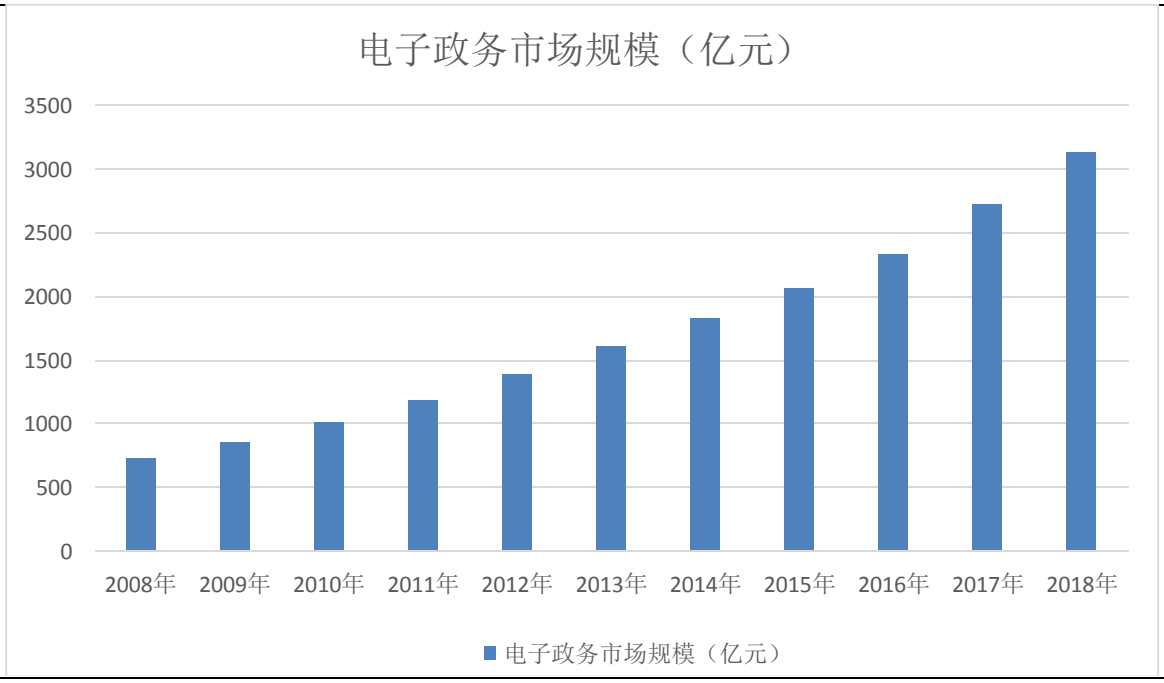
2014 年和 2016 年，卫士通全面参与了国家关于银行业的商用密码推广试点工作。通过两批应用试点示范，不仅实现了商用密码在银行业的广泛应用，也进一步验证了 SM 系列密码算法以及相关密码产品的安全性、可靠性、稳定性。此外，卫士通基本形成网络信息安全产业链。2015 年，卫士通收购了三零盛安、三零瑞通和三零嘉微，基本形成从芯片、产品到系统和应用的完整网络信息安全产业链，进一步增强市场竞争能力。同时，卫士通积极配合国家关于《密码法》、《商用密码管理条例》以及《网络安全等级保护条例》《关键信息基础设施安全保护条例》等配套法规的制修订工作，为依法规范商用密码应用提供坚实的法律基础。

2）现有党政军客户基础扎实

2017 年公司完成中央企业网络安全总体方案，承担中国电科集团整体保障任务和成员单位网站防护任务，十九大重大活动保障期间为近 30 家政府网站和央企 1300 余个网站提供安全保障服务。2018 年 1 月 26 日，卫士通公司控股股东中国网安凭借独创的“网络信息安全整体保障服务”模式，与招商局集团签署业内首个网络信息安全整体保障服务合同，开启全方位合作，共同应对网络安全新挑战。

以电子政务市场为例，2018 年其市场规模将超过 3000 亿，按照其中 IT 服务占总体投入的 30%的历史经验，其政务 IT 类服务的市场规模将达到千亿规模。

图 1：电子政务市场规模



资料来源：前瞻产业研究院，东兴证券研究所

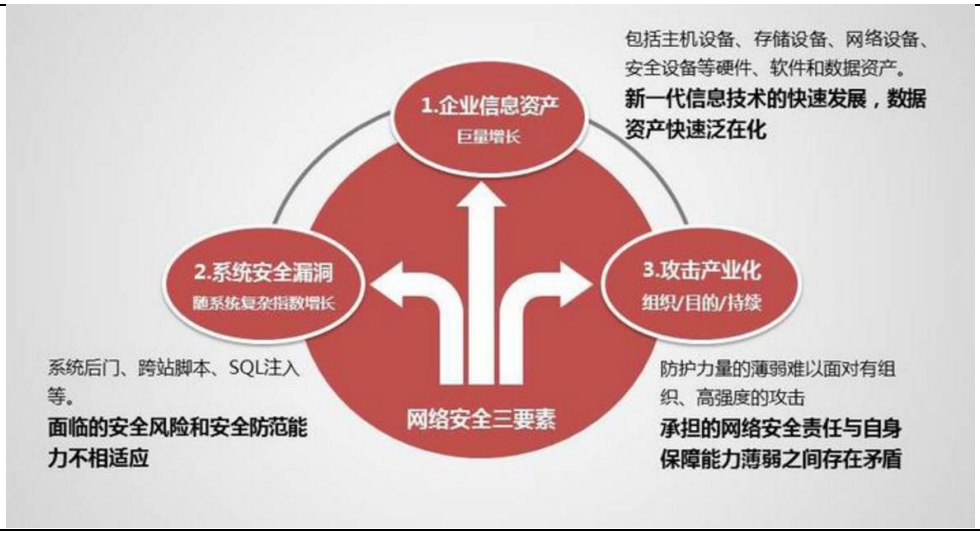
凭借公司信息安全国家队的资质，公司有望在千亿级市场中取得不俗的市场份额。

其子公司三零瑞通的核心产品加密手机的重要客户主要是国家涉密人员，如党政军人士等，拥有大约一百亿的市场空间。卫士通积极布局这一市场，2015 年 12 月 14 日，华为携手中国移动、卫士通在广州发布全球首款基于 VoLTE 通信加密解决方案的中国移动华为 Mate 8 VoLTE 安全手机。次年中国移动卫士通 4G VoLTE 安全手机(华为 Mate8 尊御版)”荣获“CITE2016 创新产品与应用奖”，2017 年包括与华为合作研发的 Mate 9 在内的 3 款安全手机已正式发布。

3）企业客户需求变化，关键信息基础设施运营单位已无法独自应对网络空间安全“新常态”

对于企业而言，在规模尚小时可以通过自己建机房并维护，解决内部无纸化、信息化问题，但随着企业规模增大业务量增加，后期的信息化投入成本、人力越来越多，且网络威胁纷繁复杂，企业和政府部门的信息系统及保障需要由专业的信息安全企业来负责。

图 2：信息系统安全三个基本维度



资料来源：中国网安，东兴证券研究所

未来从信息系统安全风险评估的三个基本维度来分析网络空间安全的新常态：

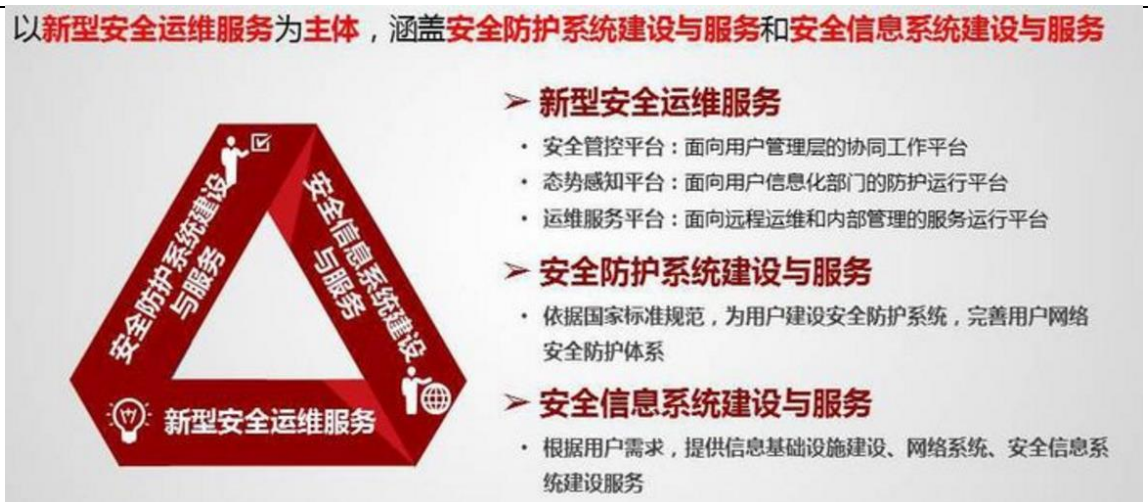
一是信息资产的总量或数据资产的总量在急剧的增加，甚至可以讲数据资产已经成为国家和企业最重要的资产。DT 时代的到来，我们要保护的对象的重要性和总量已经成指数级别增长；

二是信息系统的复杂度和关联度空前提升，系统脆弱性随之增加；

三是网络攻击已经从过去单纯的炫技，向有组织、长期持续且极具针对性的谋取商业、经济利益甚至军事、政治利益转变。

当前形势已经到了任何关键信息基础设施运营单位依托自身力量都无法承受的严峻阶段。而对于安全企业来说，未来的发展趋势应该是采取实时检测安全威胁、动态主动调整防护策略、安全事件快速应急处置等综合手段来应对日益严峻的网络安全威胁，构建全方位、全过程、全覆盖的体系化整体保障能力。

图 3：新型安全运维服务、安全防护系统建设与服务与安全信息系统建设与服务



资料来源：中国网安，东兴证券研究所

为应对新态势，卫士通公司逐步从信息安全产品向安全信息系统转变，从产品提供商向综合的信息安全服务商转变。卫士通未来有四大发展方向：一是安全产品，二是安全和信息化功能合一的产品，三是安全系统，四是做安全运维。

从安全产品提供商到安全服务整体解决方案提供商，改变了原来“产品交付”模式，做完项目就走，将安全运维交给客户去维护的弊端；也解决了企业对网络本身安全防护手段较多，但对数据安全保护较少的当前困境，提升整体防护水平。

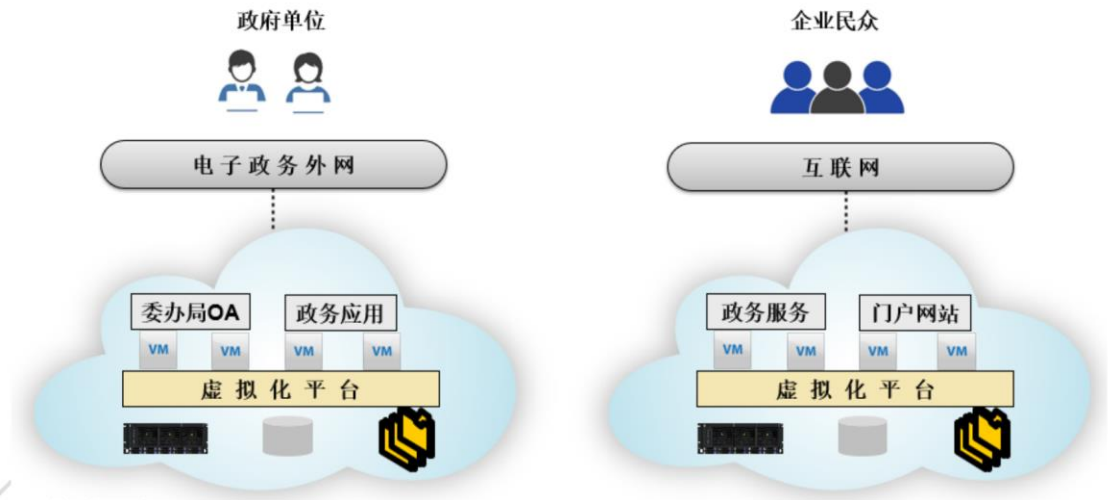
此外，此次华丽转身也将提升卫士通的盈利水平，从原来交付产品模式到每年都交运营管理费，收入更加平滑，其对下游的话语权也将提升，有效提高毛利率水平。随着传统优质央企需求的转变，公司有望迎来新一轮增长。

2. 与阿里云合作，卡位党政军云安全

2.1 政务云助力政府实现信息化升级和服务转型，当前发展迅猛

首先政务云是指云计算技术在政府行业的应用，利用云计算虚拟化、高可靠性、高通用性、高可扩展性以及快速、按需分配、弹性服务等优势，将目前已有的机房、计算、存储、安全、应用支撑、信息数据等资源统筹使用起来，为政府提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等综合服务平台，实现基于政务云的政府办公和政府服务。

图 4：政务云结构示意图



资料来源：云计算开源产业联盟，东兴证券研究所

2.1.1 传统 IT 架构制约政府信息化发展，政务云助力政府服务转型

表 1：传统 IT 与云计算对政府信息化的影响

传统 IT 制约政府信息化发展	政府使用云计算的优势

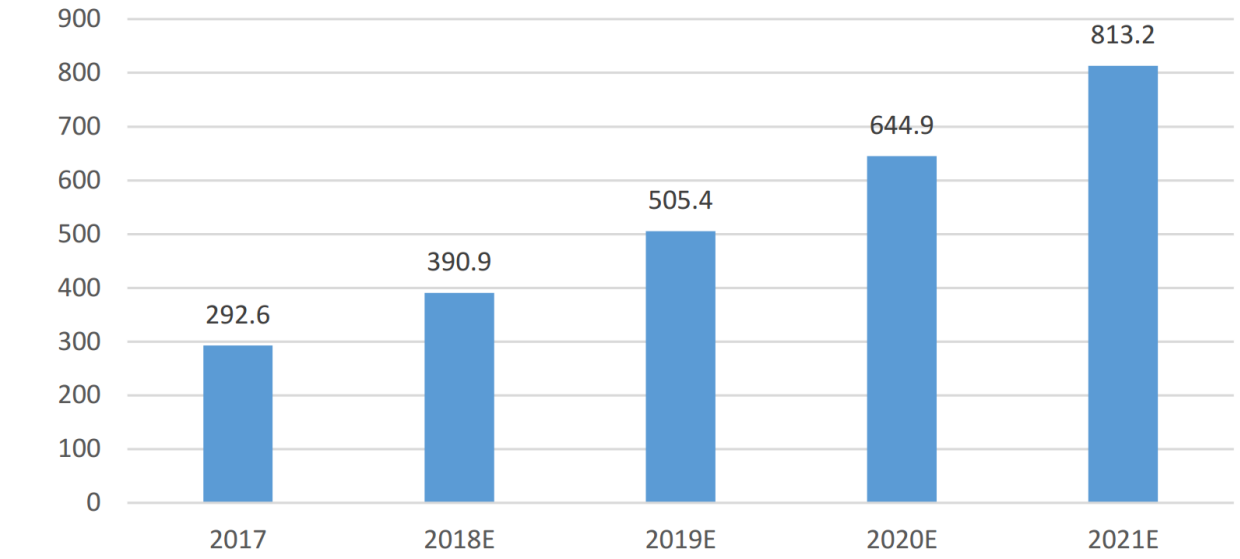
“信息孤岛”影响政府服务水平和效率	打破藩篱，“数据多跑路，群众少跑腿”，建立服务型政府
初始成本投入过高，快速扩容能力不足	促进政府信息化降成本，提效能
缺乏统一建设与规划，安全问题突出	提升政府信息化安全水平

资料来源：云计算开源产业联盟，东兴证券研究所

2.1.2 政务云前景广阔，发展迅猛

2017 年我国政务云市场增长迅猛，超过工业、金融、互联网等其他行业，达到 292.6 亿元规模，预计未来几年政府会保持稳定投入，到 2021 年市场规模将达到 813.2 亿元。

图 5：中国政务云市场规模

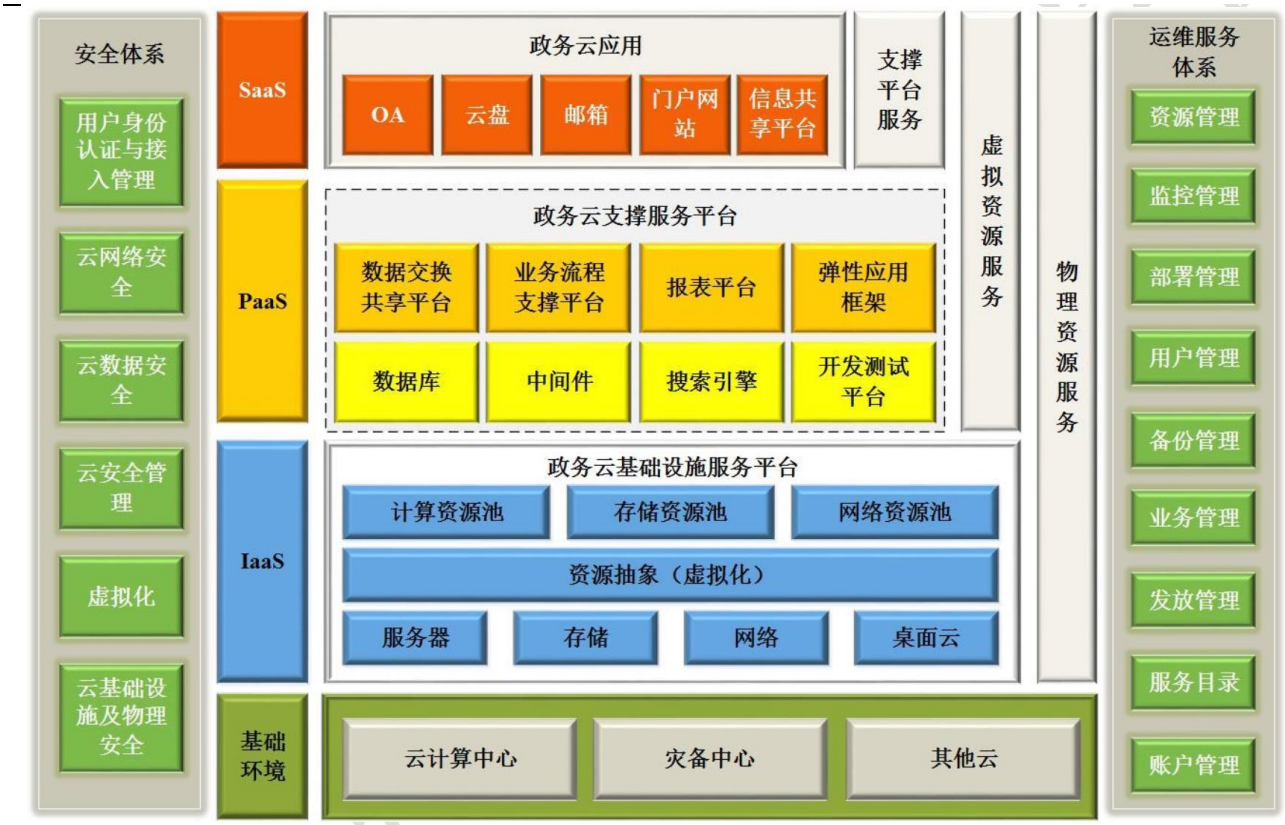


资料来源：中国政务云发展白皮书，东兴证券研究所

2.2 云计算安全问题成为政务云最大隐患

政务云建设的关键技术包括服务器虚拟化技术、分布式计算和存储技术以及网络虚拟化技术，他们共同为政务云应用提供统一的基础设施资源服务。除此之外，安全体系和运维服务体系也是政务云架构中的重要部分，这些构成了整个政务云的体系架构。

图 6：政务云体系架构



资料来源：中国政务云发展白皮书，东兴证券研究所

信息安全是决定政务云推广的关键要素。在网络安全上升到国家安全层面之后，政府行业对云计算的安全性要求，就成为了重中之重。政府使用云计算的安全隐患主要分为两个层面：一是系统的安全，包括云主机安全、中间件安全、操作系统安全、网络安全、应用安全等；二是数据的安全，在政务云数据聚集化的趋势下，集中后的数据如何安全的存储、传输和使用也是个挑战。

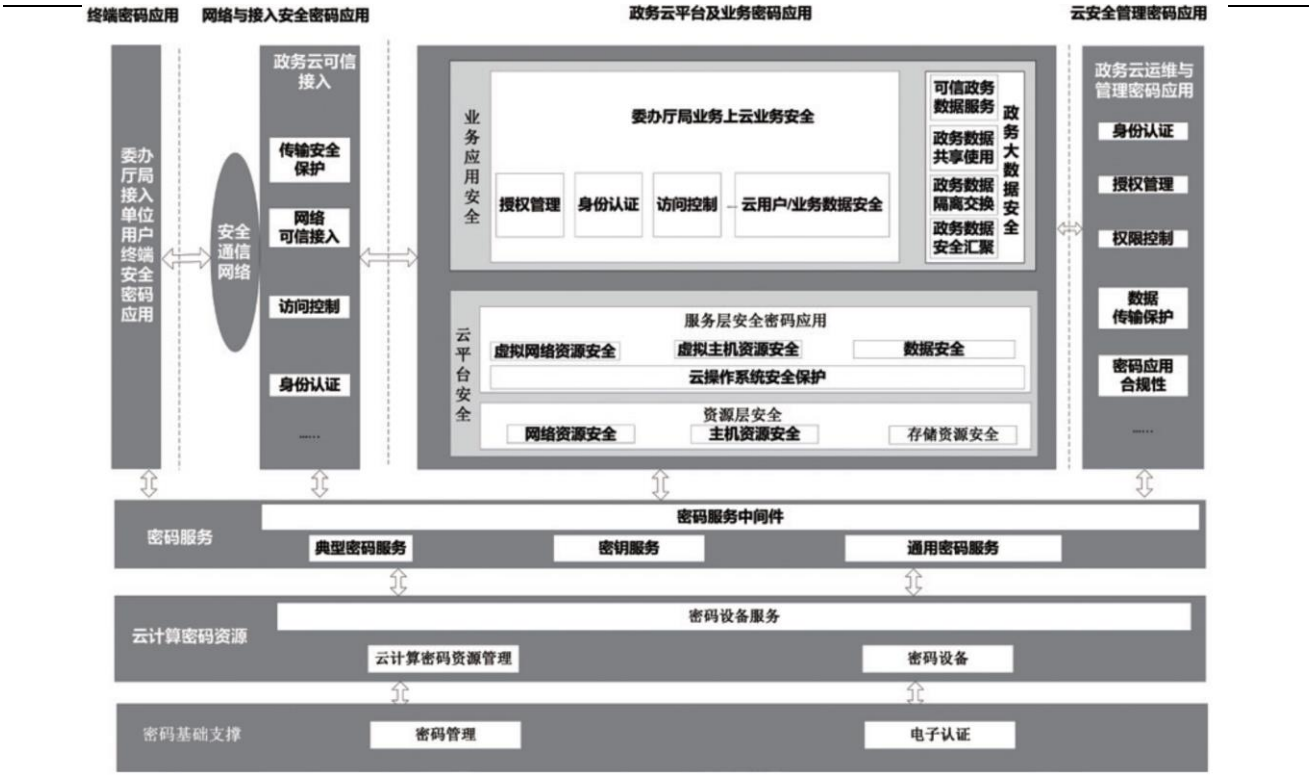
而密码技术和数据有天生的关联关系，这就像办公室里，重要的东西要放在抽屉里锁起来，数据放到云上难道就不锁起来？所以说密码它在数据生命周期是防护的技术。数据在传送的时候，可以做传送过程中的加密，端到端的加密。在数据的静态过程中，比如说存在文件服务器或者是数据库可以对它进行加密。所以它可以伴随数据的整个生命过程。密码技术非常有用，到了云里来它应该更重要，即使数据脱离了控制，仍然可以用密码主动的方式来保证数据安全。

2.3 卫士通提出政务云密码应用总体架构，为政务云安全稳定运行提供全方位保障

针对用户信息分散、业务应用身份认证方式 / 访问控制方式实现各异等突出问题，卫士通提出了政务云密码应用总体架构，采用国产商用密码在各个环节保证数据的完整性、机密性、不可抵赖和真实性，为政务云安全稳定运行提供全方位密码保障支撑，为用户安全认证、单点登录、数字签名验签等提供密码应用的技术支撑，实现政务数据在云计算环境下的安全传输、安全存储、安全流转、安全使用和安全监管，保障政

务协同和资源共享过程的可管可控可追溯，为业务应用迁移到政务云提供密码安全性保障。

图 7：政务云密码应用总体架构



资料来源：中国商用密码产业发展史，东兴证券研究所

2.4 卫士通与中国最大“阿里云”合作，打造“网安飞天”安全云

2018 年 5 月，公司控股股东中国网安与阿里云计算有限公司在杭州签署战略合作协

议，携手国内一流的国产软硬件厂商，基于国家科技重大专项核高基项目，打造国际先进、国内领先的“网安飞天”安全云平台品牌，构建国产自主可控安全云平台生态链。

此次合作是国内第一公有云平台与信息安全国家队第一品牌的强强联合。公司主要承担“网安飞天”安全云平台产品的总体及应用研究，积极参与“网安飞天”安全云平台产品的研制，并且将作为该产品的市场运营负责单位，开展“网安飞天”安全云平台在政务、国防和重点行业的应用和推广。公司具备信息安全国家队资质优势以及在央企中网络安全先进的运维经验，有望结合阿里云的技术优势，在未来党政军自主可控安全云平台中取得更大市场份额。历史来看，公司于 2014 年安全集成服务从 1.65 亿跃升为 6.96 亿，此次与阿里云强强联合，有望在安全集成领域掀起另一轮高增长态势。

党政军上云规模预计不低于 5000 朵云，如果安全服务按照 300 万的价格，其市场规模将达到 150 亿，助力公司新一轮业绩飞跃。

3. 5G 军用标准制定者，独家军用 5G 通信服务商，卡位未来网战主峰

3.1 网络空间战日益激烈，卫士通制定军用 5G 通信标准，抢占未来网战高地

5G 因为传输速率和稳定性方面有质的飞跃的特点满足未来战场通信任务需求。5G 通信系统全球部署将具有与军用通信系统相同甚至更强的服务能力。各类军用移动终端可以直接运用 5G 通信进行网络作战。

网络空间被军事战略家们称为陆、海、空以及太空以外的“第五作战空间”。近年来，随着互联网技术的迅速发展，世界多国，尤其是拥有先进技术和庞大军事预算的发达国家，纷纷下大力气组建自己的网络攻击部队。

图 8：不断加速的美国网络战备

资料来源：公开网络，东兴证券研究所

世界各国均将网络空间视为利益空间和生存空间，先后制订了前瞻性的网络空间战略，通过技术、管理和外交等方面的手段，争夺网络空间的技术优势和行动优势，在确保自身安全的同时积极建立网络空间威慑力量。网络空间面临的风险日益深化，成为全球秩序和国家安全的全新挑战。

表 2：各国在网络战部队方面的布局

供应链层面	把控基础软硬件平台
要素支撑层面	引领安全基础研究
发展模式层面	军民融合积极创新
战术布局层面	预埋系统漏洞后门
作战力量层面	强调能力建设
战略理念层面	预防对手技术突袭

资料来源：东兴证券研究所

从 2010 年以来以美国为首的 10 多个国家制定了网络空间战略。现在有超过 46 个国家已经成立了网络部队。与此同时，每年针对政府、敏感机构的网络攻击，也持续增加。尤其是在中国周边国家和地区，韩国、日本、印度都建立了庞大的网络部队，台湾也开始筹建，计划在 2019 年全面行成战斗力。我国也成立了中国人民解放军 61398

部队用于网络作战，对于网络攻防安全需求很大。

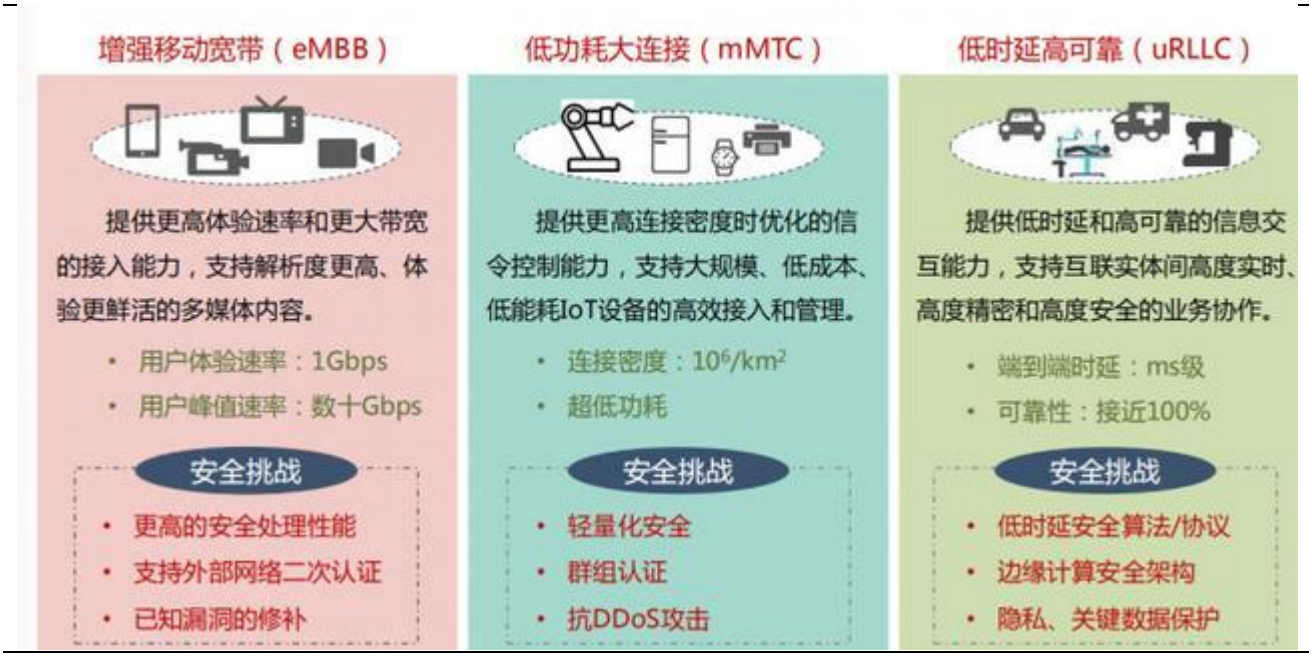
图 9：各国在网络战部队方面的布局

资料来源：公开网络，东兴证券研究所

我国 2018 年国防支出达到 11069.51 亿元人民币，比去年增加 8.1%，重点是要加强信息化建设。2020 年我国军费规模将达 12984 亿元。我国军民融合领域还有重大潜力。而同时军民融合正是中国区别于其他国家提出的“第四大 5G 应用场景”。5G 所采用的高频频谱，在我国之前一直属军用领域。卫士通是国家 03 通讯专项的 5G 安全架构的总体单位，也是军民融合 5G 高安全标准单位，给党政军提供高安全通讯专网，市场巨大。

5G 的安全机制相对于 4G 发生非常重大的变化。5G 有新的应用场景，有增强移动宽带，低功耗大连接、低时延高可靠三大应用场景。

图 10：5G 的三大应用场景以及相应的安全挑战



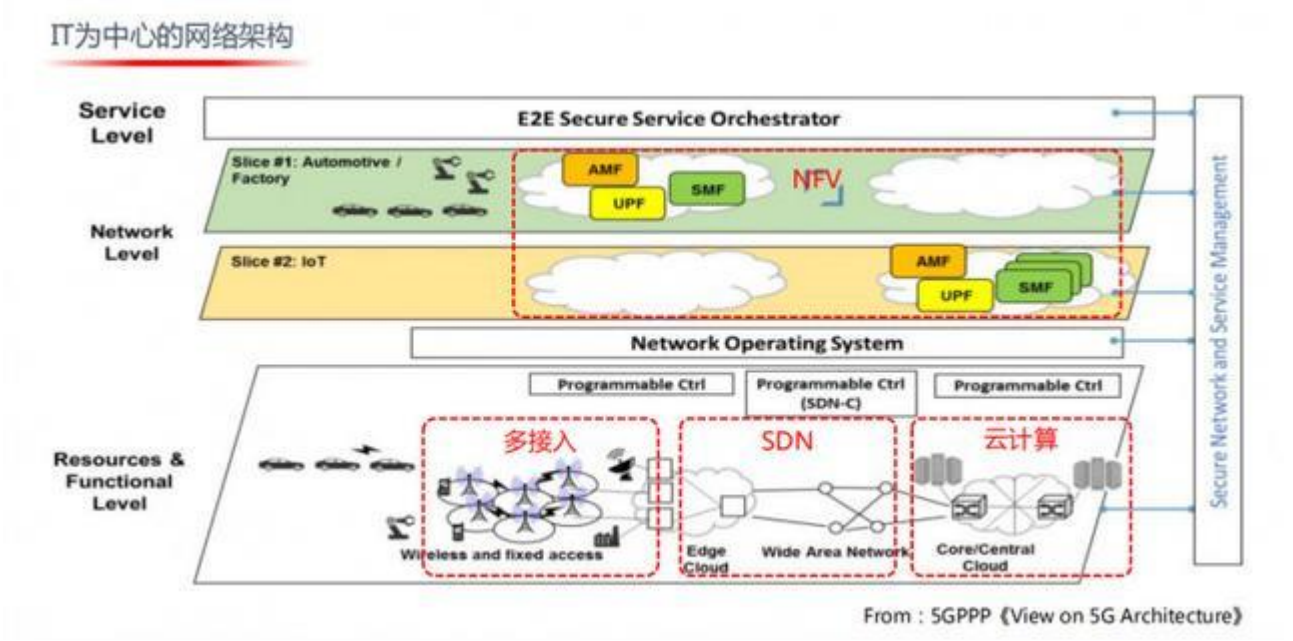
资料来源：2018 年中国网络安全大会资料，东兴证券研究所

对增强移动宽带来说，它的安全挑战需要更高的安全处理性能，这时候用户体验速率已经达到 1G；二是它需要支持外部网络二次认证，能更好地与业务结合在一起；三是需要解决目前发现的已知漏洞的问题。

对低功耗网络来说，需要轻量化的安全机制，以适应功耗受限、时延受限的物联网设备的需要；需要通过群组认证机制，解决海量物联网设备认证时所带来的信令风暴的问题；需要抗 DDOS 攻击机制，应对由于设备安全能力不足被攻击者利用，而对网络基础设施发起攻击的危险。

对于低时延高可靠来说，需要提供低时延的安全算法和协议，要简化和优化原有安全上下文的交换、密钥管理等流程，支持边缘计算架构，支持隐私和关键数据的保护。

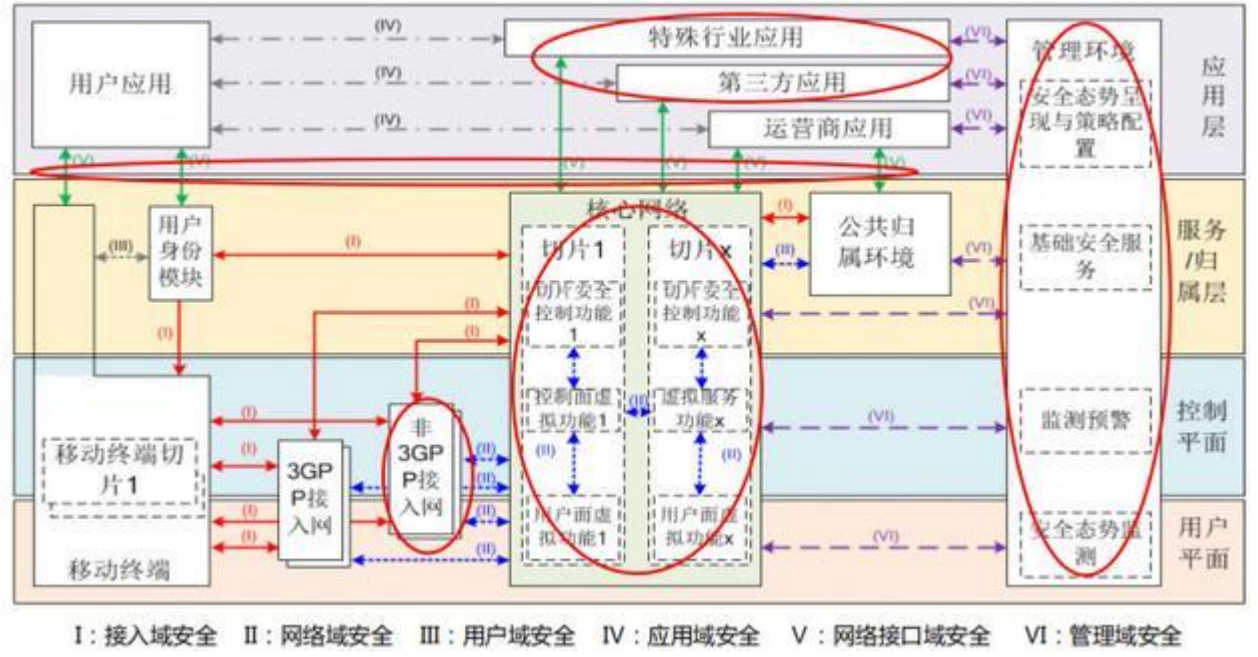
图 11：5G 应用以 IT 为中心的网络架构



资料来源：2018 年中国网络安全大会资料，东兴证券研究所

而为了更好的支持 5G 应用场景，5G 提出了以 IT 为中心的网络架构，会引入多无线接入、SDN、云计算、NFV 等技术。SDN 和 NFV 这样的技术引入，可以构建逻辑隔离的安全切片，用来支持不同应用场景差异化的需求。但这些技术个引入也对安全造成带来了巨大的挑战，由于它使网络边界变得十分模糊，以前依赖物理边界防护的安全机制难以得到应用。所以，安全机制要适应虚拟化、云化的需要。

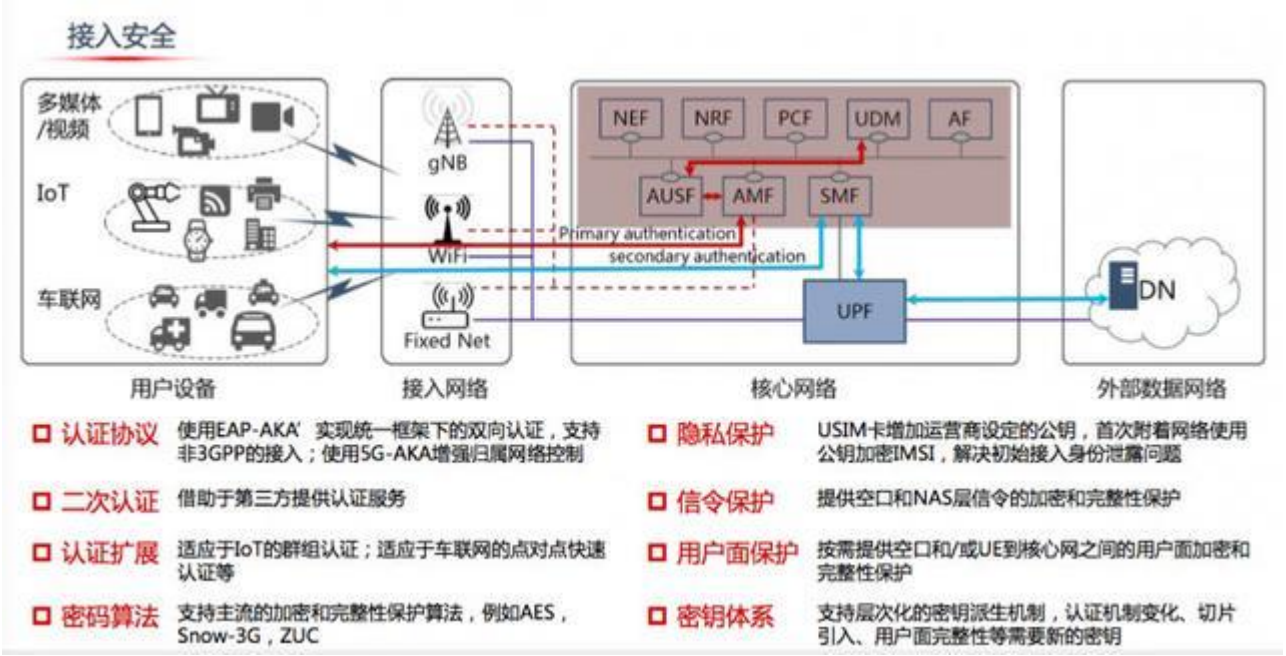
图 12：5G 安全防护架构



资料来源：公开网络，东兴证券研究所

5G 安全防护架构延用了原来 4G 安全参考架构，相比之前增加了非 3GPP 接入、切片和虚拟网元的安全、网络开放接口安全和安全管理等安全实体。

图 13：5G主要安全机制



资料来源：公开网络，东兴证券研究所

5G 的安全体制也根据 5G 使用场景进行了改进。其中比较重要的是：

1）密钥体系，算法需要支持主流的加密和完整性算法，但现在这些算法可能会在 5G 做进一步的改进，因为 5G 运营周期在 20 年，20 年之中，比如量子计算比较成熟，受到攻击的风险会增大。所以，在算法方面也可能会进行升级。在密钥体制方面，还是要支持程度化的密钥派生机制，同时能够提供由于认证机制变化，切片引入和用户面的完整性保护所需要的这些新的密钥。

2）网络安全切片方面，需要提供网络切片的安全隔离，差异化的安全服务，终端能够安全地访问切片，切片的安全管理以及内部的安全通信等等。

3）安全态势管理与监测预警方面，我们要借助于，位于各种网络功能以及安全设备类的安全探针，采用标准化的安全设备统一管控接口对安全事件进行上报，下发统一的安全策略，可以进行深度学习、机器学习手段来嗅探和攻击的检测，应对未知的安全威胁。同时，根据安全威胁能智能化生成相关的安全策略调整，并将这些策略调整下发到各个安全设备中，从而构建起一个安全的防护体系。

4）隐私保护方面，现在对个人信息保护非常关注的，5G 里上面承载着很多用户的隐私和敏感信息，包括用户的号码，用户位置信息等等，我们可能需要从技术和管理两个途径进行保护，在技术方面，加密传输和加密存储，访问控制，对关键隐私数据在网络传输中进行匿名。

而 5G 应用安全则涉及集中场景。

1）5G 环境下终端安全。

图 14：5G 终端安全需求

资料来源：公开网络，东兴证券研究所

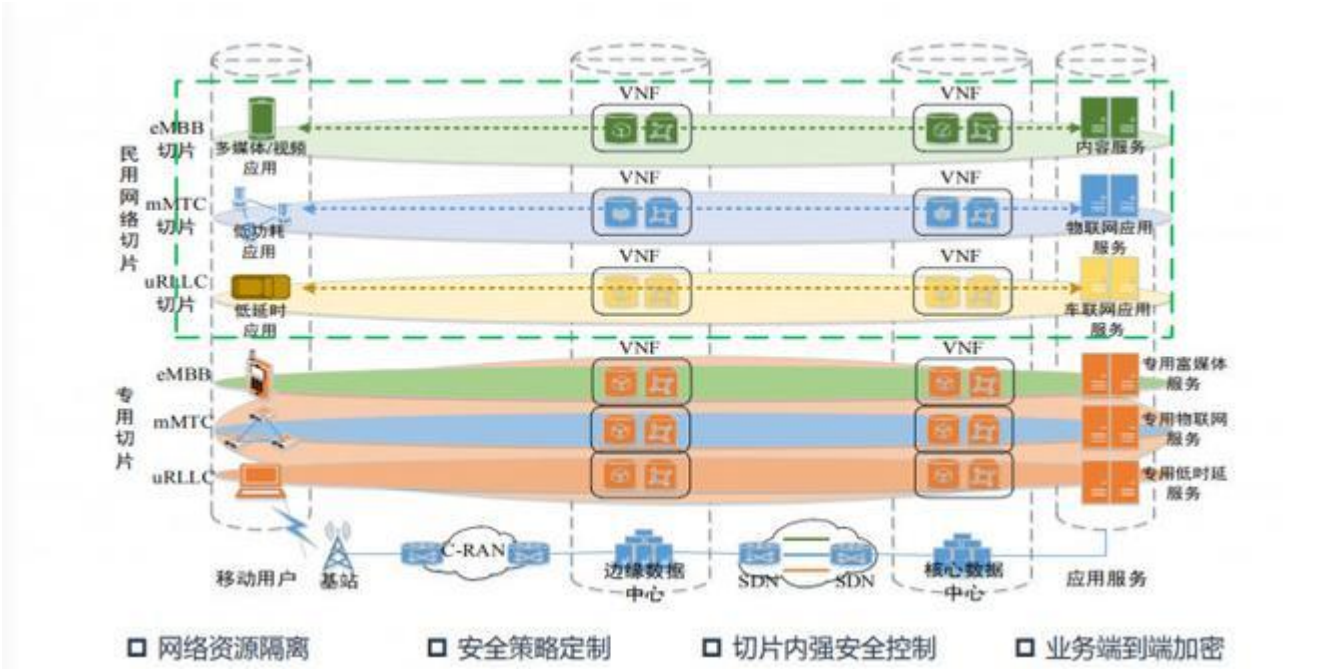
5G 环境下，终端安全应该是云端协同防御的体系，在终端方面需要从硬件层、系统层、应用层几个层次考虑相应的安全防护措施，同时我们可以借用云端，借用网络能力提供更多的网络安全支持，包括端到端加密，数据安全存储，因为网络带宽足够，一些敏感区域不一定要存在终端上，可以存在云端。云端形成的安全监测预警。的现在用的比较多的基于云端的远程管控，应用安全和系统安全的支撑等等。

2）面向行业垂直领域的安全服务，如政务云等。

对各种垂直行业来说，业务应用、安全威胁和安全需求存在很大的差异。我们可以依托 5G 网络基础设施，基于前面服务化的思想，在统一架构下为垂直行业提供定制性和差异化的安全能力。具体来说，我们可以对网络里的安全资源，密码算法、5G 认证协议和安全知识库，对安全资源进行抽象和封装，对外提供安全服务，对加密传输服务提供认证服务、信用服务、入侵检测服务等等，这些服务会通过网络能力开放引擎，开放给各种应用，这样就可以使应用在使用网络通道的同时也可以获得网络提供的安全服务，能够更高效、更安全地实现信息服务。

3）安全行业专网建设。

图 15：5G 下安全专网建设

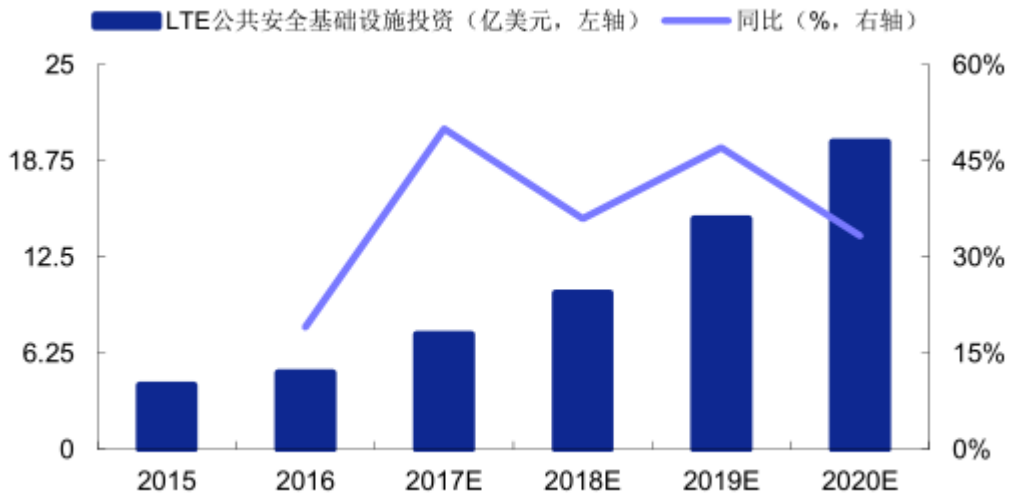


资料来源：公开网络，东兴证券研究所

对国防、政务、公共安全和关键行业，对安全有着特别的要求，包括高安全业务可靠保护、敏感信息安全存储与受控访问、特殊用户隐私保护、特殊行业运营管理。特殊行业在 4G 以前是基于运营商的公共基础网络，在上面构造了专网的技术来实现，这种方式投资成本是比较高的，建设周期比较短，同时可扩展性、灵活性也存在不足，它的技术体制难以跟上发展，通信系统本身进展是很快的，我们往往可以看到系统已经进入到 4G，但很多专网还停留在 2G、3G 上。5G 现在开放性架构和灵活性的应用，为构建行业特定专网提供了新的解决思路。对于一般性的安全行业，对安全的需求进行定义，5G 网络可以提供差异化的安全服务，可以定制和优化获得想要的安全能力。对安全要求更高的行业来说，可以将满足自己安全需求的能力、功能进行事例化，通过服务接口编排到网络切片当中，形成自己的专业高安全切片。

2020 年全球公共安全领域 LTE 专网设备投资将达到 20 亿美元，年平均复合增长率为 40%。

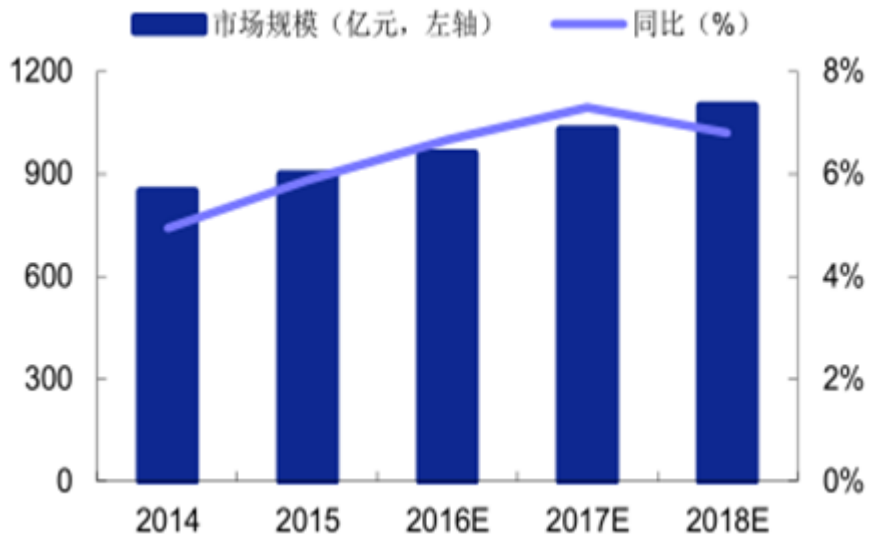
图 16：全球公共安全领域 LTE 专网设备投资规模及增速



资料来源：公开网络，东兴证券研究所

根据预测，未来全球专网通信市场将继续保持稳定的增长趋势，行业规模有望在 2018 年达到 1100 亿元。

图 17：全球专网通信市场规模及预测



资料来源：公开网络，东兴证券研究所

中国专网市场， 2011 年至 2016 年专网市场规模复合增长率约为 19%，2016 年市场规模已达到 121 亿元，同比增长约 19.8%。中国专网市场的增速高于全球市场增速。

图 18：中国专网市场规模

图表：中国专网市场规模

资料来源：公开网络，东兴证券研究所

3.2 布局 5G 物联网市场，5 亿研发投入

同时，卫士通布局 5G 物联网安全市场。中国电信股份有限公司北京研究院发布的《2017 物联网安全研究报告》阐述，物联网已渗透到我们的生活、消费等各个领域，Gartner 显示，2017 年全球物联网设备数量将达到 84 亿，首次超过全球人口数量(75 亿)，同时，到 2020 年，全球物联网设备将达到 204 亿。而从 2017 年以来，物联网恶意软件对物联网设备发起的攻击比去年同期相比增长了 280%，物联网僵尸网络规模不断扩大，并加速进入威胁扩张期。到 2020 年在企业发现的攻击中将有超过 25%跟物联网有关，针对物联网安全的措施在安全预算所占比例却低于 10%物联网安全既是挑战也是机遇。2020 年全球物联网的安全市场将从 2015 年的 68.9 亿美元增长至 289 亿美元，即 2015 年至 2020 年的复合年增长率（CAGR）为 33.2%，未来市场巨大。

公司曾经获得四川政府关于物联网方向的专项资金 300 万元,子公司三零瑞通曾于获得了国家给予的 300 万元和 200 万元的资助用于物联网的研究。此外，卫士通加盟成都物联网产业发展联盟，还成立了物联网课题组专门针对物联网的安全威胁、安全架构、安全体系等安全问题进行分析研究，承担了国家相关课题的研究项目；在物联网部分试点项目中，卫士通承建了“平安重庆”信息安全保障系统建设、“智慧武汉”、“西部智谷”等项目安全保障体系设计工作，为物联网的信息安全体系发展提供了技术及服务支撑。根据卫士通 17 年年报，在 2017 年又专门成立了物联网安全专项推进组，并在 3 月 22 日募集了 17,687.74 万元投入到物联网的系列安全芯片项目，后续将达到 51,250 万元。

3.3 商用密码将是 5G 安全核心技术，公司深耕多年战略卡位优势明显

商用密码对于网络空间技术领域具有重要的基础性、引领性、关键性地位，特别是在数据加密、身份鉴别、访问控制、取证溯源等方面依然发挥着难以替代的重要作用。所以商用密码技术作也被做为未来网络安全核心支撑技术重点发展。而 5G 网络多样化的应用和新架构新技术对密码算法应用提出了新的需求。

卫士通作为一家以密码技术为基点的公司，在商密依领域默默耕耘二十余年，奠定了商密行业绝对龙头地位。卫士通提前进行技术战略卡位，成立 5G 安全专项推进组，重点开展 5G 密码应用等研发，依托于密码技术这一核心优势，确立以密码为基础的统一信任体系，构建多元分立的数据防护模型,建立整体性的安全服务基础设施,形成面向垂直行业的 5G 安全解决方案，未来无疑会给企业带来积极影响。

4. 布局“量子密码”，卡位量子通信领域

4.1 军工信息化已提升到国家战略高度，2018 年我国军事通信及信息化市场规模将达到千亿级别

C4ISR（军用通信指控专网）是集指挥（command）、控制（control）、通信（communication）、计算机（computer）、情报（intelligence）及监（surveillance）与侦察（reconnaissance）等功能为一体的现代化军事通信指挥控制系统，是国防信息化战略的关键。从国际视野来看，美国军事通信工业能力极强，已建成全球最先进的 C4ISR（军事指挥控制通信专网），能满足美国军方各种通信的需求从市场规模来看根据 Frost&Sullivan 的统计数据，美国 1999 年 C4ISR 市场规模达到 109.5 亿美元，同比增长 27.1%。到 2012 年，美国 C4ISR 市场规模达到 755.3 亿美元。

而我军信息化建设正处于快速发展的关键时期,“信息系统一体化、武器装备信息化、信息装备武器化、信息基础设施现代化”是我国国防工业发展的战略方向。随着未来我国军事通信技术的升级换代，预计我国军费采购将迅速增长，实现对军事电子通信领域的市场需求。我国 C4ISR 尚处于起步阶段，距离全链条产品普遍成熟还有较大差距。由于有国际先进技术作为参考，我国 C4ISR 的高速发展期比美国要短，预计未来将有 3-5 年的 25%以上增速的高速增长阶段,2013 年我国国防开支为 7202 亿元，按国防开 10%-15%增长测算，C4ISR 占比 2018 年提升到美国 2012 年的水平(11.1%)，则 2018 年我国 C4ISR 相关开支将近 1440 亿元。军用专网基本上都需要加密，未来也会采用量子通信加密保证绝对安全。

表 3：军事通信市场规模测算

时间	C4ISR 占国防支出	C4ISR 相关支出
2010	4.5%	315 亿元
2013	6.5%	473 亿元
2018E	11%	1440 亿元

资料来源：中国产业信息网，东兴证券研究所

4.2 量子通信行业发展前景广阔长期市场规模将超过千亿

量子通信是指利用量子纠缠效应进行信息传递的一种新型的通讯方式。相较于传统的密码学，拥有无条件安全性和对窃听者的可检测性。在传统的密码学研究中，通讯对象必须事先确定密钥，密钥交换先于信息传输，因而容易被破解。量子通信可以克服经典通信被窃听的风险，从而大大提高通信安全系数，量子通信可视作单模光纤两端加上能代替常用光模块功能的、光量子态的发送和接收设备，实现基于物理加密的保密通信。量子通信相比经典通信还有时效性高、传输速度快、抗干扰能力强、传输能力强等优点。

图 19：量子通信绝对安全实现原理

资料来源：公开网络，东兴证券研究所

我国量子通信技术和产业化水平处于世界领先水平，将挑起大国信息安全战略的重担。据前瞻产业研究院发布的《量子通信行业发展前景与投资战略规划分析报告》数据显示，2017 年，我国量子通信行业市场规模达到了 180 亿元，到 2018 年将达到 320 亿元左右，同比增长 77.78%，预计到 2024 年，我国量子通信行业建设及运营服务市场规模达 912 亿元，同比增长 13.57%。根据预测，国内量子通信短期市场规模在

100-130 亿元左右，长期市场规模将超过千亿。

图 20：2017-2024 年中国量子通信市场规模及增长情况

资料来源：前瞻产业研究院，东兴证券研究所

图 21：量子通信政策

时间	文件	内容
2017, 5	科技部、教育部、科学院、国家自然科学基金委员会关于印发“十三五”国家基础研究专项规划的通知	面向多用户联网的量子通信关键技术和成套设备，率先突破量子保密通信技术，建设超远距离光纤量子通信网，开展星地量子通信系统研究，构建完整的空地一体广域量子通信网络体系，与经典通信网络实现无缝链接
2017, 11	发改委关于组织实施2018年新一代信息基础设施建设工程的通知	提出国家广域量子保密通信骨干网络建设一期工程
2018, 3	政府工作报告肯定量子通信发展成果	将量子通信与载人航天、深海探测、大飞机并列为重大创新成果，认可量子通信行业地位和发展成果

资料来源：公开网络，东兴证券研究所

4.3 提早布局量子密码，中国网安走到世界前列

卫士通大股东中国网安也已经早早布局、开展“量子密码”的相关研究。依托中国电科 30 所侧重信息安全建设领域，资料显示，早在 2012 年 12 月 20 日，中国电科就与中科院签署了战略合作框架协议，双方约定在量子计算、太赫兹技术、纳米技术、空间技术以及信息学、现代计算学等方面开展前沿技术探索研究。

4.3.1 申报国家自然科学基金项目，彰显研发实力

2017 年，由中国网安三十所徐兵杰博士主持申报的国家自然科学基金面上项目“量子真随机数产生协议设计、分析及实现技术研究”和黄伟博士主持申报的国家自然科学基金青年科学基金项目“实用化量子安全多方计算协议理论研究”双双获批立项。国家自然科学基金作为我国支持基础及前沿科技研究的国家级科研项目，并且 2017 年申请量达到历史最高的 190840 项，竞争激烈程度史上空前，由此可见脱颖而出的必然是极其具有技术含量。2017 年度中国电科共获批国家自然科学基金项目 15 项（包括重大科学仪器项目 1 项，面上项目 2 项，青年科学基金项目 12 项），中国网安获资助项目总数在中国电科成员单位中位居第二位。不仅如此，“量子真随机数产生协议设计、分析及实现技术研究”项目是中国网安首次获批国家自然科学基金“面上项目”。而相较于青年科学基金评审要求不同的是，“面上项目”不但要求申报的项目具有重要的科学意义和研究价值，更要求项目组整体在相关领域都具有较深厚的研究积淀和较强的科研实力。该项目的获批代表着中国网安在量子密码研究领域所取得的技术地位，具有标志性意义。

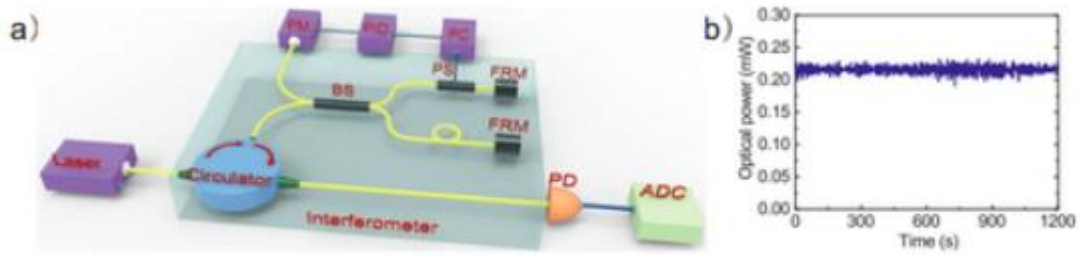
图 22：申报国家自然科学基金项目

资料来源：公开网络，东兴证券研究所

4.3.2 发布新型高速量子随机数发生器，入选 2017 国防科技工业十大新闻

密钥是密码安全性的根基，而密钥产生的质量如何、效率高低，则取决于随机数产生的技术，即随机数发生器的性能的好坏。通俗来讲，随机数产生的速率越高，就意味着在单位时间内能够产生更多的钥匙、做到真正意义上的‘随机发钥’，令企图窃密的人眼花缭乱、无‘钥’可用，难以在保密通信中迅速找到破解密码的钥匙并窃密，具备理论上的完美安全性。作为量子保密通信核心设备之一，量子随机数发生器的发展已经成为保障一个国家实现量子保密通信成功与否的重要关键。

图 23：量子随机数发生器



资料来源：公开网络，东兴证券研究所

2017 年中国网安发布量子保密通信领域的最新究成果——新型高速量子随机数发生器。这款由中国网安研发的新型高速量子随机数发生器，实现实时产生速率大于 5.4 G 比特每秒，极限值突破 117G 比特每秒，刷新了此前中国科学技术大学团队研制的 68Gbps 的高速量子随机数发生器记录，成为目前世界上产生速率最高的量子随机数发生器。中国网安研制的新型高速量子随机数发生器具有真随机、超速率、小型化等特点，是目前唯一在理论上被严格证明能产生完全不可预知随机序列、接近理想真随机的随机数产生技术，研发团队已经获得 5 项发明专利，实时量子随机数比传统技术高 3~4 个量级，处于国际领先水平，有望成为新一代高速高安全物理噪声源，可广

泛应用于量子通信产业和信息安全产业。立足需求、量体裁衣。针对不同的设备需求，中国网安还推出了设备级、小型化、光电一体小型化等系列高速量子随机数发生器。其中，最小的高速量子随机数发生器仅有手机大小，采用光电路一体化设计，适配 USB 3.0 接口，实时产生速率超过 1.4 Gbps，体积小、稳定性高，在国际同类产品中优势明显。后续，由中国网安研发的系列量子随机发生数产品，将有望广泛应用在国防、党政、金融、能源、工业基础设施等信息系统网络空间信息安全、保密通信、身份认证、大型国民经济统计分析等领域，创造出重要的应用和产品价值。

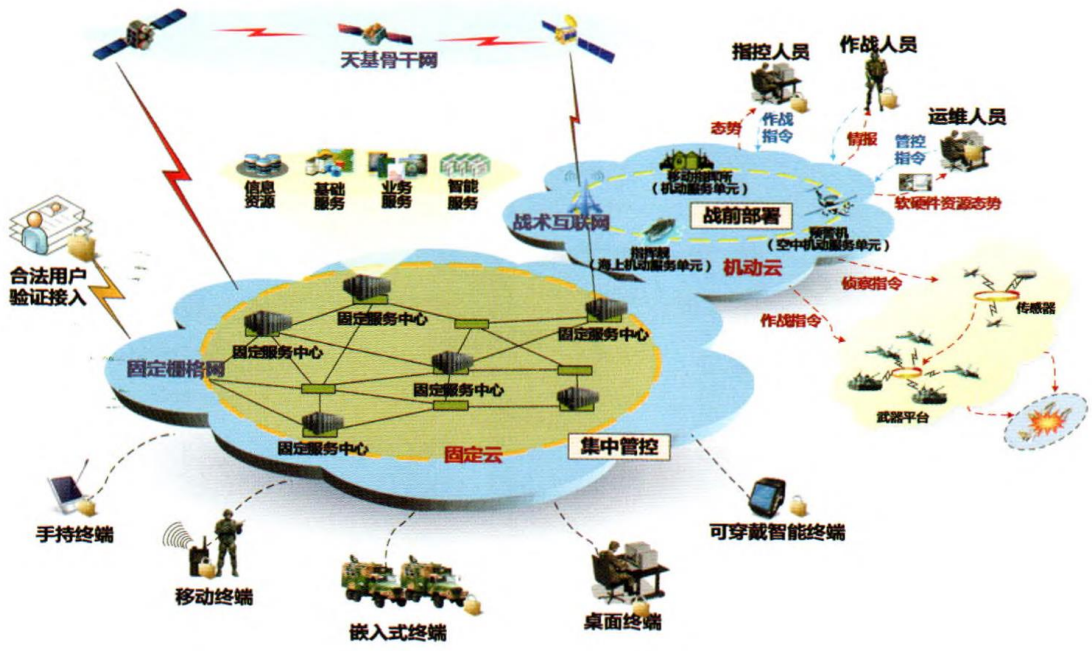
5. 未来战争中信息安全成为重中之重，卫士通提供综合信息安全体系

5.1 作战云将是未来信息化基础，我国需要追赶美军脚步

5.1.1 美军引领全球军事新动向，已经在军事领域应用云计算技术

美军从国防部、军种多个层次都对云架构进行了运用，提出联合信息环境(JIE)、作战云、战术薄云等概念，JIE 通过整合全军共用的数据、服务形成统一共享的运行和使用环境，为敏捷系统构建提供支撑，带动 C4ISR 系统整体发展和体系化作战能力的提升打造坚实的基础平台；作战云、战术薄云则是美空军、海军在战术层次的组织运用构想。

图 24：未来军事信息系统概念范畴



资料来源：《基于云架构的军事信息系统概念及机理研究》，东兴证券研究所

战略云是指为美军在美国大陆与海外各基地、港口、场站、兵营等永久军事设施提供各类保密或非保密语音、视频、数据服务的通信网络．这些网络通常采用固定的光纤

骨干网(带宽达 100mb / s)，连接到中央管理的服务器 / 路由器集群设备，这些集群设备又接入全球信息栅格，由统一的网络集成中心和网络战与安全中心进行管控。

战术云与战略云有很大区别，这从根本上决定了战术云在参与构建联合信息环境过程中的特殊性．本质上讲，战术云是一种临时网络，不能依托永久的网络设施，而总是在严苛的战场环境下临时构设．在具体实施过程中，信号连在旅信号参谋军官的战术控制下行动，而旅信号参谋军官负责作战指挥服务器的操作与维护。

5.1.2 作战云的必要性

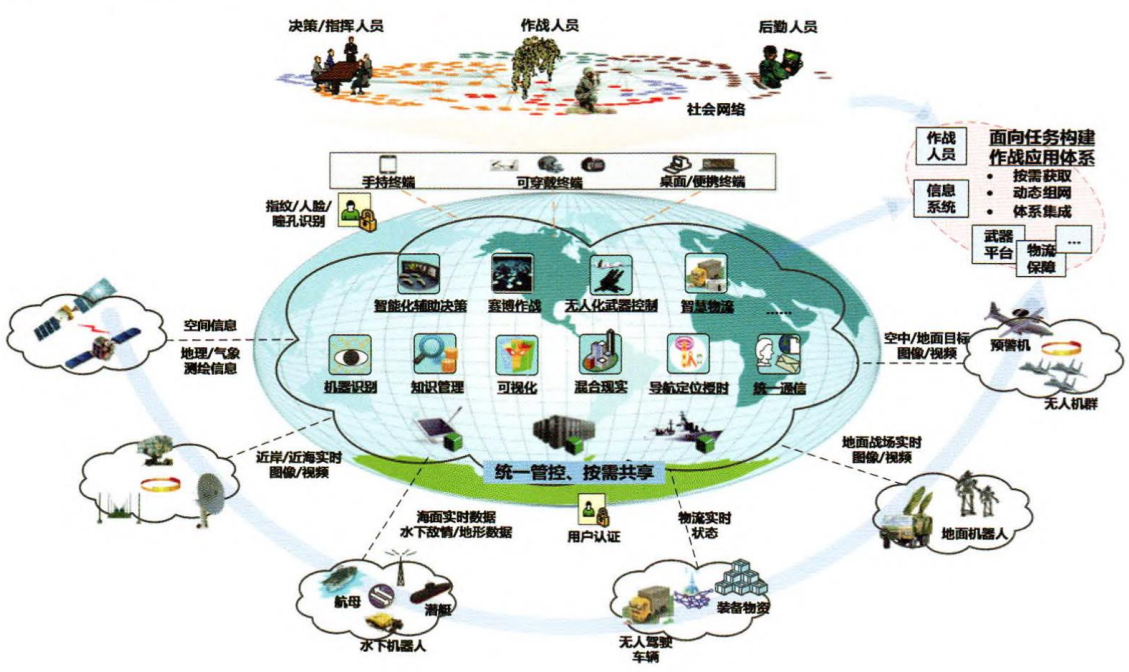
发展作战云的必要性源于 3 个“动”：

1）打击目标的动态性不断提高．现代战争无导不成战，就以导弹为例，其作战能力已从打击固定目标，打击时敏目标，向打击移动目标拓展；

2）武器平台的动态性不断提高．仍以导弹为例，已从固定阵地发射向无依托机动发射转变，从固定弹道到机动弹道转变；

3）作战环境的动态性不断提高．信息化作战条件下，敌情、我情、战场环境瞬息万变．上述变化，将引发作战样式、指挥模式、保障模式的一系列变革，从而对信息化作战体系提出了新的更高的要求。

图 25：未来作战云技术架构设想

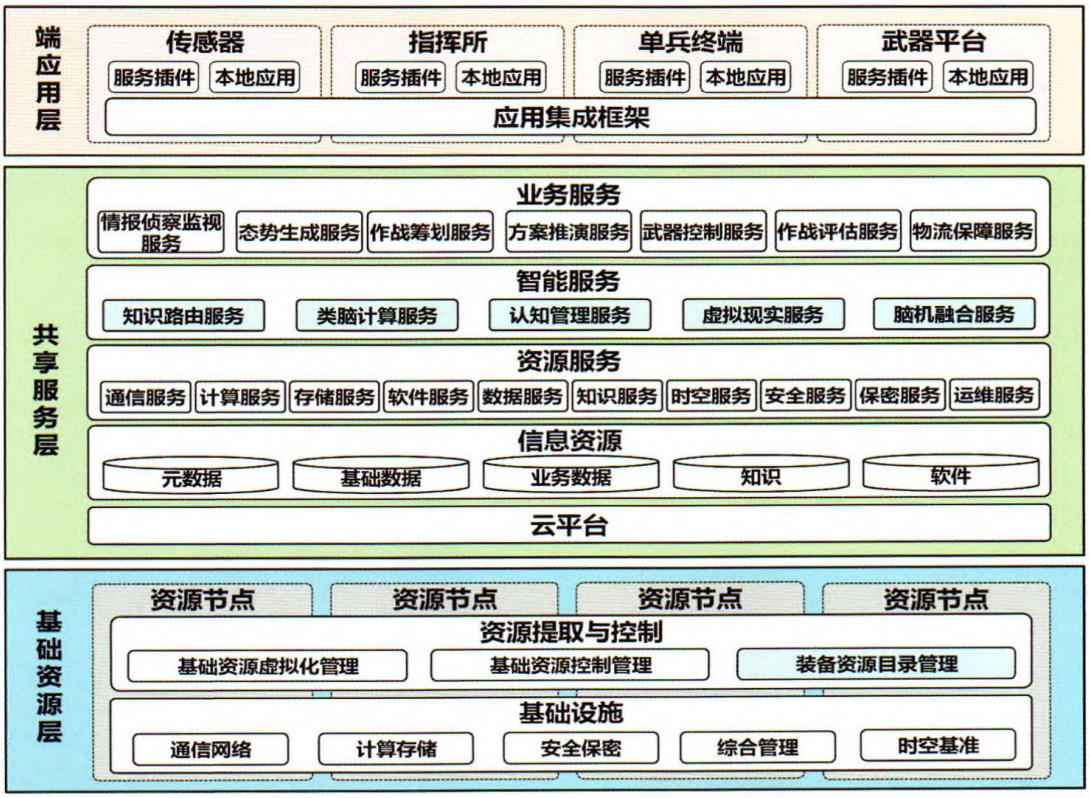


资料来源：《基于云架构的军事信息系统概念及机理研究》，东兴证券研究所

单纯系统集成、网络集成式的体系架构只是信息化作战体系发展的初级阶段，因为每个系统、每个网实质仍是小而全的系统，背后是条块分割的组织机构，很难真正围绕作战融合成为有机的体系，从而无法实现无缝的协同和联合．必须升华为网络信息体

系，因为网络主要解决“联”的问题，信息解“用”的问题，体系才能解决“强”的问题。

图 26：未来作战云技术架构设想



资料来源：《基于云架构的军事信息系统概念及机理研究》，东兴证券研究所

5.2 作战云化后对信息安全提出了新的要求，卫士通将为军队提供国内最强防护

未来战争中军队面临各方面的信息化打击，其中有几种最为致命：1. 瘫痪云基础设施；2. 通讯端泄密；3. 数据链乃至数据库遭到袭击；4. 电子干扰。任何一种打击成功，对军队的安全都将是致命的。

而卫士通作为 A 股唯一信息安全国家队，将肩负起为我国军事信息安全保驾护航的责任。公司目前与阿里云合作，在云安全方面有望成为国内第一梯队；旗下三零瑞通的核心产品安全手机的用户主要是国家涉密人员，如党政军人士等，有力保障通讯终端安全；而公司以信息加密起家，母公司中国网安目前在量子加密方面走在世界前列，在数据加密方面将有力保障军队信息安全；公司所在的中电科集团中在电子干扰方面具备多年深厚背景，具备雄厚的技术积累，与卫士通共同打造军用综合信息安全体系。

盈利预测及估值

我们预计公司 2018 年、2019 年和 2020 年，收入分别为 30.14 亿元、52.27 亿元和 76.92 亿元，归母净利润分别为 2.45 亿元、5.47 亿元和 8.08 亿元，EPS 分别为 0.29 元、0.65 元和 0.96 元，首次覆盖给与公司“强烈推荐”评级。

风险提示

安全运维推广不达预期，政务云竞争激烈，5G 应用进度低于预期。

表 4:公司盈利预测表

资产负债表					单位:百万元	利润表					单位:百万元
	2016A	2017A	2018E	2019E	2020E		2016A	2017A	2018E	2019E	2020E
流动资产合计	2,019.64	3,932.38	4,894.83	7,089.87	9,126.40	**营业收入**	1,798.90	2,137.11	3,014.53	5,227.44	7,692.93
货币资金	402.90	1,745.62	1,646.44	1,045.49	1,538.59	**营业成本**	1,164.75	1,382.68	2,022.25	3,277.18	4,775.59
应收账款	1,087.87	1,616.09	2,272.46	4,470.61	5,452.78	营业税金及附加	15.46	20.31	33.02	46.40	67.65
其他应收款	193.28	199.07	279.92	550.68	671.66	营业费用	177.34	215.34	281.33	487.85	717.94
预付款项	55.41	68.49	129.60	150.48	260.93	管理费用	270.65	330.23	461.55	800.36	1,177.85
存货	192.50	210.97	445.77	618.52	932.39	财务费用	5.57	-12.19	-23.05	-20.28	-2.47
其他流动资产	28.66	25.34	25.34	25.34	25.34	资产减值损失	47.47	74.60	0.00	0.00	0.00
非流动资产合计	1,471.02	1,640.55	1,614.46	1,585.45	1,498.36	公允价值变动收益	0.00	0.00	0.00	0.00	0.00
长期股权投资	25.00	26.61	26.61	26.61	26.61	投资净收益	1.87	1.80	0.00	0.00	0.00
固定资产	268.05	265.66	245.01	224.37	1,307.43	**营业利润**	119.53	127.96	244.90	620.53	943.25
无形资产	10.48	70.50	65.17	115.24	106.99	营业外收入	76.54	50.01	59.07	59.07	59.07
其他非流动资产	0.00	54.55	54.55	54.55	54.55	营业外支出	0.00	0.00	0.00	0.00	0.00
资产总计	3,490.67	5,572.93	6,509.29	8,675.32	10,624.75	**利润总额**	196.07	177.97	303.97	679.60	1,002.32
流动负债合计	1,917.78	1,185.13	1,863.12	3,451.49	4,548.95	所得税	23.11	19.47	45.60	101.94	150.35
短期借款	828.56	0.00	0.00	411.98	483.58	**净利润**	155.75	150.30	245.01	547.78	807.90
应付账款	801.80	1,077.00	1,670.85	2,782.21	3,706.90	少数股东损益	17.20	8.20	13.36	29.88	44.06
预收款项	40.26	59.54	167.27	151.41	313.24	归属母公司净利润	155.75	150.30	245.01	547.78	807.90
一年内到期的非	0.00	0.00	0.00	0.00	0.00	EBITDA	40.16	75.02	50.80	24.29	15.65
非流动负债合计	0.00	0.00	0.00	0.00	0.00	**EPS（元）**	0.19	0.18	0.29	0.65	0.96
长期借款	0.00	0.00	0.00	0.00	0.00	**主要财务比率**					
应付债券	0.00	0.00	0.00	0.00	0.00		2016A	2017A	2018E	2019E	2020E
负债合计	1,917.78	1,185.13	1,863.12	3,451.49	4,548.95	**成长能力**					
少数股东权益	83.81	92.01	105.37	135.25	179.32	营业收入增长	12.2%	18.8%	41.1%	73.4%	47.2%
实收资本（或股	432.52	838.34	838.34	838.34	838.34	营业利润增长	-9.3%	7.1%	91.4%	153.4%	52.0%
资本公积	300.31	2,558.35	2,558.35	2,558.35	2,558.35	归属于母公司净利润	4.7%	-3.5%	63.0%	123.6%	47.5%
未分配利润	756.24	899.10	1,144.11	1,691.89	2,499.80	**获利能力**					
归属母公司股东	1,572.89	4,387.80	4,646.17	5,223.83	6,075.80	毛利率(%)	35.3%	35.3%	32.9%	37.3%	37.9%
负债和所有者权	3,490.67	5,572.93	6,509.29	8,675.32	10,624.75	净利率(%)	9.6%	7.4%	8.6%	11.1%	11.1%
现金流量表					单位:百万元	总资产净利润（%）	5.77%	2.97%	4.94%	5.68%	5.36%
	2016A	2017A	2018E	2019E	2020E	ROE(%)	10.5%	3.5%	5.4%	10.8%	13.7%
经营活动现金流	-137.05	-50.85	-174.83	-1,073.54	373.17	**偿债能力**					
净利润	155.75	150.30	245.01	547.78	807.90	资产负债率(%)	54.9%	21.3%	28.6%	39.8%	42.8%
折旧摊销	31.00	36.88	26.09	29.01	87.10	流动比率	1.05	3.32	2.63	2.05	2.01
财务费用	5.57	-12.19	-25.08	-9.78	2.80	速动比率	0.95	3.14	2.39	1.87	1.80
应收账款减少	-422.28	-534.01	-1,244.30	-730.32	-2,407.11	**营运能力**					
预收帐款增加	-59.25	19.28	107.73	-15.86	161.83	总资产周转率	0.61	0.47	0.50	0.69	0.80
投资活动现金流	-634.11	-180.76	50.21	50.21	50.21	应收账款周转率	1.85	1.58	1.38	1.38	1.38
公允价值变动收	0.00	0.00	0.00	0.00	0.00	应付账款周转率	6.71	8.04	13.73	21.07	5.27
长期股权投资减	-8.21	-1.60	0.00	0.00	0.00	**每股指标（元）**					
投资收益	1.87	1.80	0.00	0.00	0.00	每股收益(最新摊薄)	0.19	0.18	0.35	0.44	0.55
筹资活动现金流	733.25	1,578.72	25.44	422.38	69.72	每股净现金流(最新	-0.16	-0.06	-0.21	-1.28	0.45
应付债券增加	0.00	0.00	0.00	0.00	0.00	每股净资产(最新摊	1.78	5.12	5.42	6.07	7.03
长期借款增加	0.00	0.00	0.00	0.00	0.00	**估值比率**					
普通股增加	0.00	405.81	0.00	0.00	0.00	P/E	105.39	109.21	67.00	29.97	20.32
资本公积增加	6.44	2,258.04	0.00	0.00	0.00	P/B	11.02	3.82	3.61	3.23	2.78
现金净增加额	-37.90	1,347.12	-99.18	-600.95	493.10	EV/EBITDA	40.16	75.02	50.80	24.29	15.65

分析师简介

陆洲

北京大学硕士，军工行业首席分析师。曾任中国证券报记者，历任光大证券、平安证券、国金证券研究所军工行业首席分析师，华商基金研究部工业品研究组组长，2017 年加盟东兴证券研究所。

王习

香港理工大学硕士，四年证券从业经验，曾任职于中航证券，长城证券，2017 年加入东兴证券军工组。

研究助理简介

张高艳

清华大学工学硕士，2 年制造型企业运营管理咨询经验，2016 年加盟东兴证券研究所，重点关注航空智能制造、军民融合等方向。

张卓琦

清华大学工业工程博士，3 年大型国有军工企业运营管理培训、咨询经验，2017 年加盟东兴证券研究所，关注新三板、军工领域。

分析师承诺

负责本研究报告全部或部分内容的每一位证券分析师，在此申明，本报告的观点、逻辑和论据均为分析师本人研究成果，引用的相关信息和文字均已注明出处。本报告依据公开的信息来源，力求清晰、准确地反映分析师本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与，未来也将不会与本报告中的具体推荐或观点直接或间接相关。

风险提示

本证券研究报告所载的信息、观点、结论等内容仅供投资者决策参考。在任何情况下，本公司证券研究报告均不构成对任何机构和个人的投资建议，市场有险，投资者在决定投资前，务必要审慎。投资者应自主作出投资决策，自行承担投资风险。

免责声明

本研究报告由东兴证券股份有限公司研究所撰写，东兴证券股份有限公司是具有合法证券投资咨询业务资格的机构。本研究报告中所引用信息均来源于公开资料，我公司对这些信息的准确性和完整性不作任何保证，也不保证所包含的信息和建议不会发生任何变更。我们已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

我公司及其所属关联机构可能会持有报告中提到的公司所发行的证券头寸并进行交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。本报告版权仅为我公司所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用、刊发，需注明出处为东兴证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。

本研究报告仅供东兴证券股份有限公司客户和经本公司授权刊载机构的客户使用，未经授权私自刊载研究报告的机构以及其阅读和使用者应慎重使用报告、防止被误导，本公司不承担由于非授权机构私自刊发和非授权客户使用该报告所产生的相关风险和责任。

行业评级体系

公司投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，公司股价相对于同期市场基准指数的表现为标准定义：

强烈推荐：相对强于市场基准指数收益率 15%以上；

推荐：相对强于市场基准指数收益率 5%～15%之间；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

回避：相对弱于市场基准指数收益率 5%以上。

行业投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，行业指数相对于同期市场基准指数的表现为标准定义：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率介于-5%～+5%之间；

看淡：相对弱于市场基准指数收益率 5%以上。