东兴证券 DONGXING SECURITIES

布局军用云计算，打造业务新成长极

——卫士通（002268）深度报告

2018 年 09 月 19 日

强烈推荐/维持

卫士通 | 深度报告

报告摘要：

美军信息基础设施变革，指明了我军 IT 技术设施演进方向。美军从 20 世纪 20 年代以开发半自动化防空指挥控制系统为起点，开始了平台化的军事信息基础设施建设。美军信息基础设施从平台为中心，到网络为中心，再到以信息为中心，反映了上世纪 90 年代通信技术的大发展以及当前云计算、大数据、人工智能技术对传统 IT 基础设施的变革，是以技术进步引领的作战理念的转换，对我军信息化发展有非常重要的参考作用，也指明了我军 IT 基设施发展演进方向。

军事信息系统对云计算是刚需，美军青睐云计算龙头产品。随着军队信息化建设的快速发展，各部门因为自身业务的需要建立了大量军事信息系统的“烟囱”，一体化联合作战信息互联互通时出现数据共享困难的问题；且在未来信息化战场环境下大量传感器的部署，大量的实时数据只能通过云计算来解决；而保证信息安全共享的需求完全可以通过基于云计算的统一的网络防御架构，以及云计算架构逻辑上集中、物理上分散的分布式的特点来实现。

安全是云计算在军事领域应用第一要务，加强国产化和构建面向云计算的新型安全技术是有效策略。军事云计算不同于民用云计算的特点为军事云计算工作在复杂电磁环境和强网络对抗的环境之下，对于信息安全保密具有极高的要求。公司多年耕耘的加密领域将成为云计算安全技术的核心，实现完全自主可控。我们认为未来国内关键领域中使用国产 IT 巨头产品的比例将逐渐提升，不再像以前存在效率和安全的权衡问题，尤其是对安全高度敏感的军事领域的 IT 基础设施建设。

卫士通有望军工领域取得新成长极。首先，与国内云计算龙头阿里云合作，打造“网安飞天”安全云切入军工领域，有望结合国内公有云龙头阿里云的技术优势，在我军未来新一轮 IT 基础设施建设中取得最大的市场份额；其次，公司是 5G 军用标准制定者，未来有望成为独家军用 5G 通信服务商；且近期 IBM 宣布量子计算机三年后落地，将对当前密码技术造成极大冲击，而卫士通为保持加密领域领先优势，早早布局量子加密技术，保持我军信息安全。

盈利预测与估值：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，维持“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。

财务指标预测

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：张卓琦

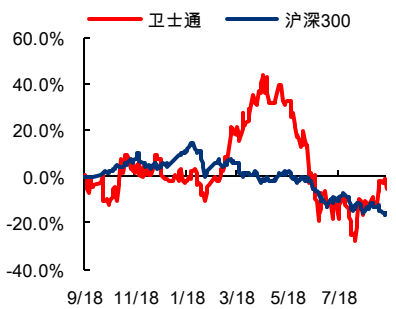
010-66554018 Zhangzq_yjs@dxzq.net.cn

执业证书编号: S1480117080010

交易数据

52 周股价区间（元）	22.1-23.1
总市值（亿元）	185.27
流通市值（亿元）	178.99
总股本/流通股（非限售）（百万股）	83834/80990
流通 B 股/H 股（万股）	1.48

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、《国防军工行业事件点评：混改东风一日起联通之后看军工》2017-08-16

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. 美国军事信息基础设施变革

军事信息基础设施的概念最早出现于美国，称之为国防信息基础设施（defense information infrastructure， DII)。军事信息基础设施是在整个军事行动范围内，满足用户信息处理和传输需求的通信网络、计算机、基础软件、应用程序、数据库、武器系统接口、数据安全服务以及其他服务的互联网络系统。

一般情况下，军事信息基础设施是指军兵种共用的信息基础设施，不包括军兵种专用的信息基础设施。军事信息基础设施所占的比重越大，军事信息系统一体化的水平越高。

军事信息基础设施由陆、海、空、天基的公共数据资源、通信基础设施、计算机基础设施、领域应用程序、基础设施运行管理和相关政策标准等构成，能在整个军事行动范围内根据作战人员、政策制定人员和保障人员的要求收集、处理、存储、分发和管理信息。

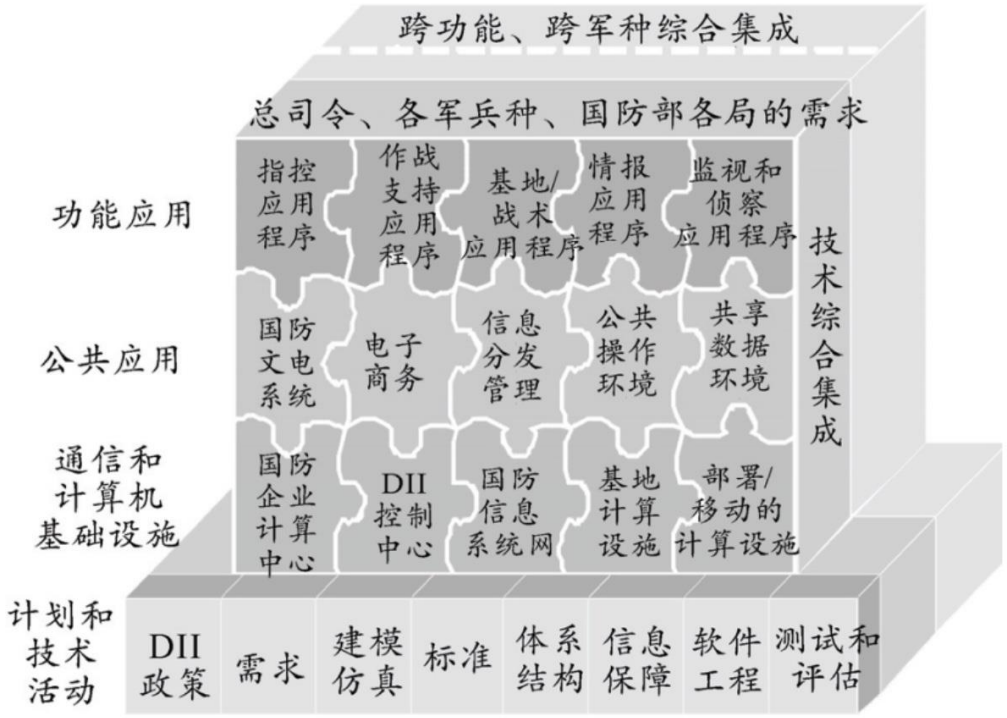
1.1 《国防信息基础设施总计划 1.0 版》

美军从 20 世纪 20 年代以开发半自动化防空指挥控制系统为起点，开始了军事信息基础设施建设。

20 世纪 90 年代初，美国开始调整军事战略，强调多军兵种联合作战。 1991 年的海湾战争暴露出美军的信息系统缺乏互连、互通、互操作性，无法提供作战空间的统一图像，适应不了联合作战的需要，并且存在严重的重复建设现象，浪费大量人力物力。

1992 年，美国参谋长联席会议提出了“武士”C4I 计划，作为美国军事一体化信息系统发展的总目标。在“武士” C4I 概念的指导下， 1992 年美国国防部在《国防管理报告决议》中做出了建设国防信息设施的决定， 1993 年 1 月正式批准，不久发表了**《国防信息基础设施总计划 1.0 版》**。

图 1：国防信息基础设施的参考模型



资料来源：《国防信息基础设施总计划 1.0 版》，东兴证券研究所

总计划规定了信息基础设施的主要组成、作用、责任，并成为跟踪其向服务环境发展的工具。

1）计划与相关技术活动：

国防信息基础设施的基础组件包括：政策、需求、建模仿真、标准、体系结构、技术基础、软件工程、测试评估、联合频谱管理以及信息保障；

2) 通信和计算机基础设施:

国防信息基础设施的通信与计算机基础设施提供信息处理与传输服务，使作战人员获得无缝的连通性，无论何时何地，都能接入并获取进攻、防御以及用于执行任务的信息。

3) 公共应用:

公共应用所提供的能力用于所有的职能与组织。它通过国防文电系统，为个人或部门提供跨组织、跨功能、跨地域的信息传输能力，并利用电子商务、电子数据交换支持电子商务，如采购、供应、运输及付费等。

4) 功能应用:

功能应用涵盖国防部所有的应用领域，依靠公共应用程序为职能机构提供共享信息的环境； 同时，功能应用程序也依靠通信和计算机基础设施的信息处理和传输能力为职能机构提供服务。

1.2 全球信息栅格(GIG)

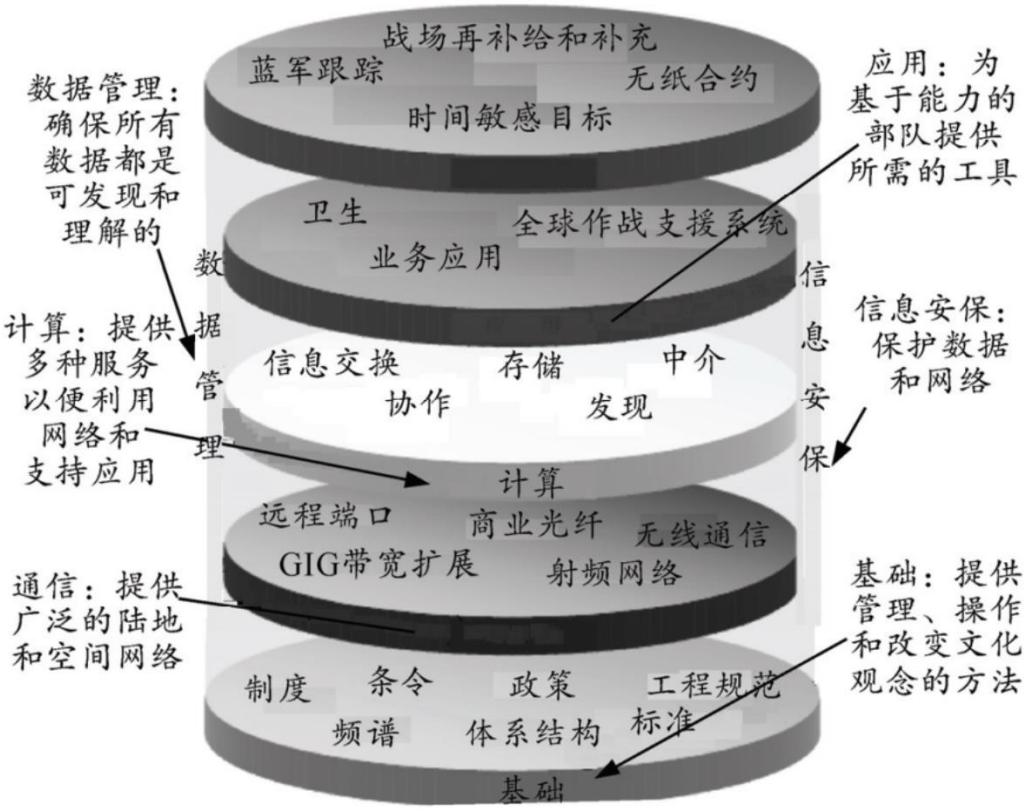
1999 年起，美国国防部主抓并开始建设全面支持“网络中心战”的新一代信息基础

设施——全球信息栅格(global information grid， GIG)，计划到 2020 年实现，以取代平台中心时代的国防信息基础设施。

全球信息栅格的定义和范围：全球信息栅格是为搜集、处理、存储、发布和管理战斗员、决策者及支持人员所需信息的全球互联的端对端的信息能力、相关过程和人员的集合。

全球信息栅格包括美国国防部全部拥有和租用的通信计算机系统及服务软件(包括应用软件)、数据、保密业务和其他为达到信息优势所必须的相关业务。全球信息栅格任务包括国家安全和全军的战术、战役和战略的使命和职能，还与盟国及非国防部用户对接。

图 2：全球信息栅格分层结构



资料来源：网络资料，东兴证券研究所

GIG 涵盖了 DII 的基础层、通信和计算机基础设施层、公共应用层、功能域应用层中的绝大部分要素。其中：基础、通信和计算机基础设施完全相同，而 GIG 的任何用户都可使用的 GIG 的核心企业服务对应 DII 的公共应用层； GIG 的核心企业服务之上的领域服务和专业团体服务对应 DII 的功能域应用。

图 3：GIG 与 DII 的比较

GIG 中的项目	对应 DII 中的项目
基础：条令、政策	基础层：政策、需求
通信层和计算层：提供陆地网络和空间网络：提供信息处理和存储服务	通信和计算机基础设施：为公共应用、功能域应用提供信息处理服务与传输服务
核心企业服务层：提供任何用户都可使用的服务	公共应用层：提供跨功能、跨组织的能力
专业团体服务：提供事务处理和作战处理服务	功能域应用：为 C2 应用、战斗支持应用、战术应用、情报应用和监视与侦察应用，提供服务

资料来源：网络资料，东兴证券研究所

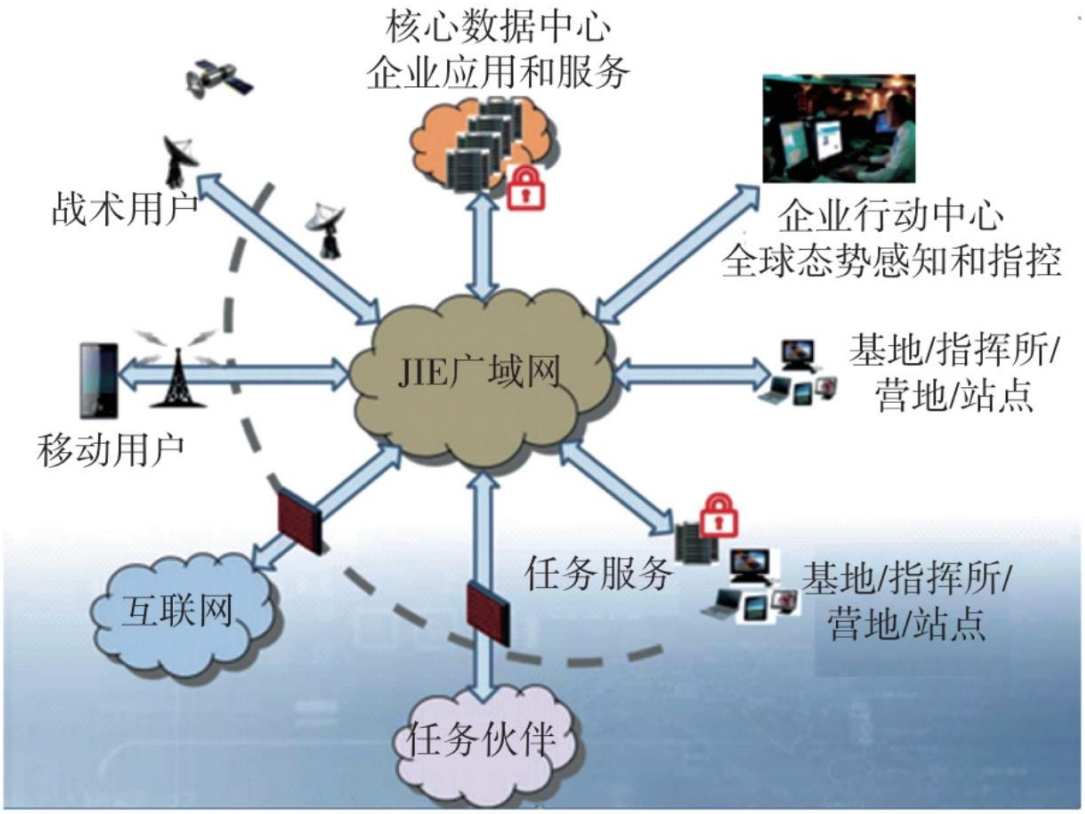
1.3 联合信息环境(JIE)

2013 年 1 月，美国参谋长联席会议主席发布了关于《联合信息环境(JIE)的白皮书》，要求美军采取措施调整现有信息处理方式，包括信息系统的结构、功能及其使用，面对联合作战需求，应用新技术对现有信息基础设施进行现代化改造，克服国防信息基础设施的不足。

GIG 是美军为“网络中心战”建设的重要基础设施，而联合信息环境是美军基于安全性考虑，对整个 GIG 重新设计而提出一个概念，它将成为 GIG 之后下一代战略储备，也将成为赛博空间发展的基础设施。现在，联合信息环境已成为美国信息系统局的一大战略目标。

JIE 将使国防部的通信和能力标准化，由标准的运行中心(包括 GEOC/EOC)和数据中心(主要是 CDC 核心计算数据中心)来管理，**通过单一的安全性堆栈保证安全性**，通过通用的访问能力(由 IdAM 实现)来访问，在交叉域和任务合作伙伴之间实现不受限的、安全的、全移动的访问，由通用的政策和 TTPs 来管理。

图 4：美军拟构建的 JIE 示意图



资料来源：网络资料，东兴证券研究所

JIE 主要具有以下能力特征：

1) 从网络中心化向数据中心化解决方案的过渡；
2) 快速地分发和使用集成的云服务；
3) 相互依存的信息环境，提供实时的赛博态势感知；
4) 可测量性和灵活性；
5) 安全的、弹性的和可合并的框架；
6) 通用的标准和可操作的 TTPs；
7) 加强动态的身份识别和访问管理工具。

1.1.1 为什么要对 GIG 进行改造，设计 JIE？

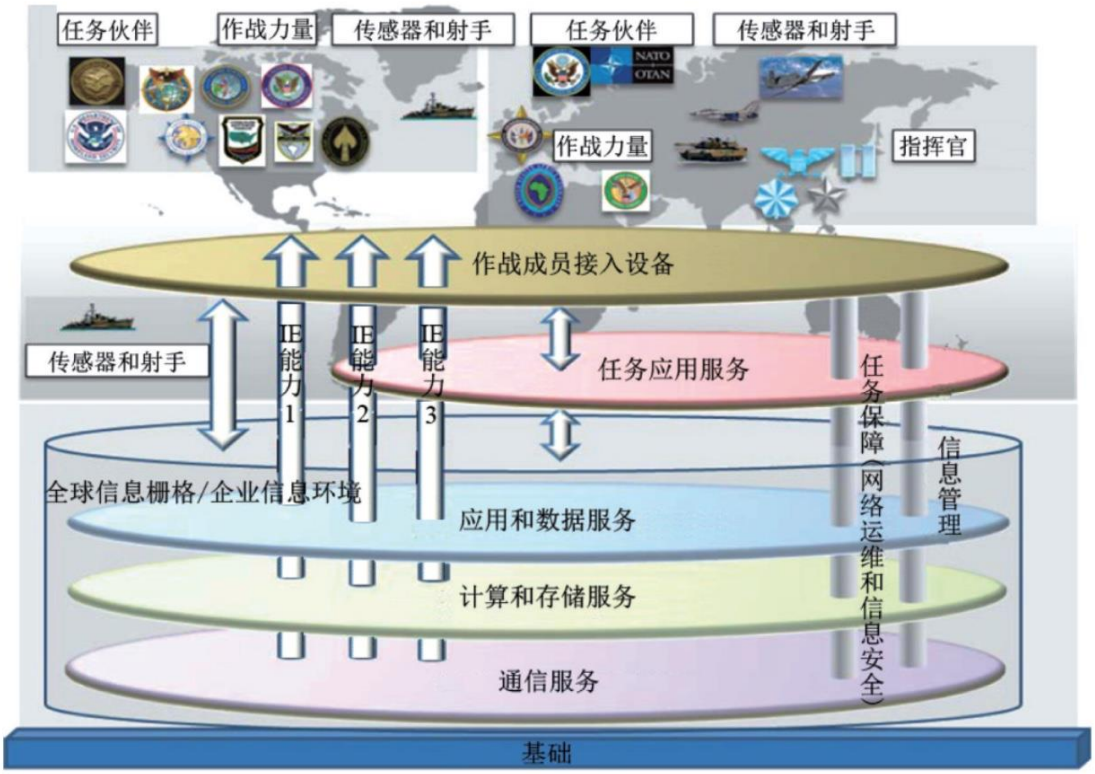
1.3.1.1 “全球一体化作战”理念的要求

“联合作战顶层概念：联合部队 2020”从顶层对早期提出的联合行动、联合功能和联合介入等概念进行了统合，设计了包含全球机动作战、全球火力战、全球网络战和全球特种作战在内“全球一体化作战”的新作战概念。

2014 年 3 月，美国国防部发布新版《四年防务评估报告》提出，将“全球一体化作战”作为美军未来发展的重点方向。“全球一体化作战”构想各种部队要素能够根据全球化的态势及时进行合成，实现横跨各个领域、梯队、地理界限以及组织架构的协

同，作战部队拥有更强大的能力在赛博空间的通用环境里去观察、去理解、去战斗、去防御。

图 5：信息体系联合信息环境构想



资料来源：网络资料，东兴证券研究所

正是这种作战方式的变革要求，才促使美军必须对其指挥控制的经络体系做出革命性的调整，从而构建一个任务指挥型的信息环境，将指挥艺术与控制科学相结合．实现对信息技术、战斗和网络安全快速集成，满足快速变动的条件要求，为此提出了联合信息环境计划。

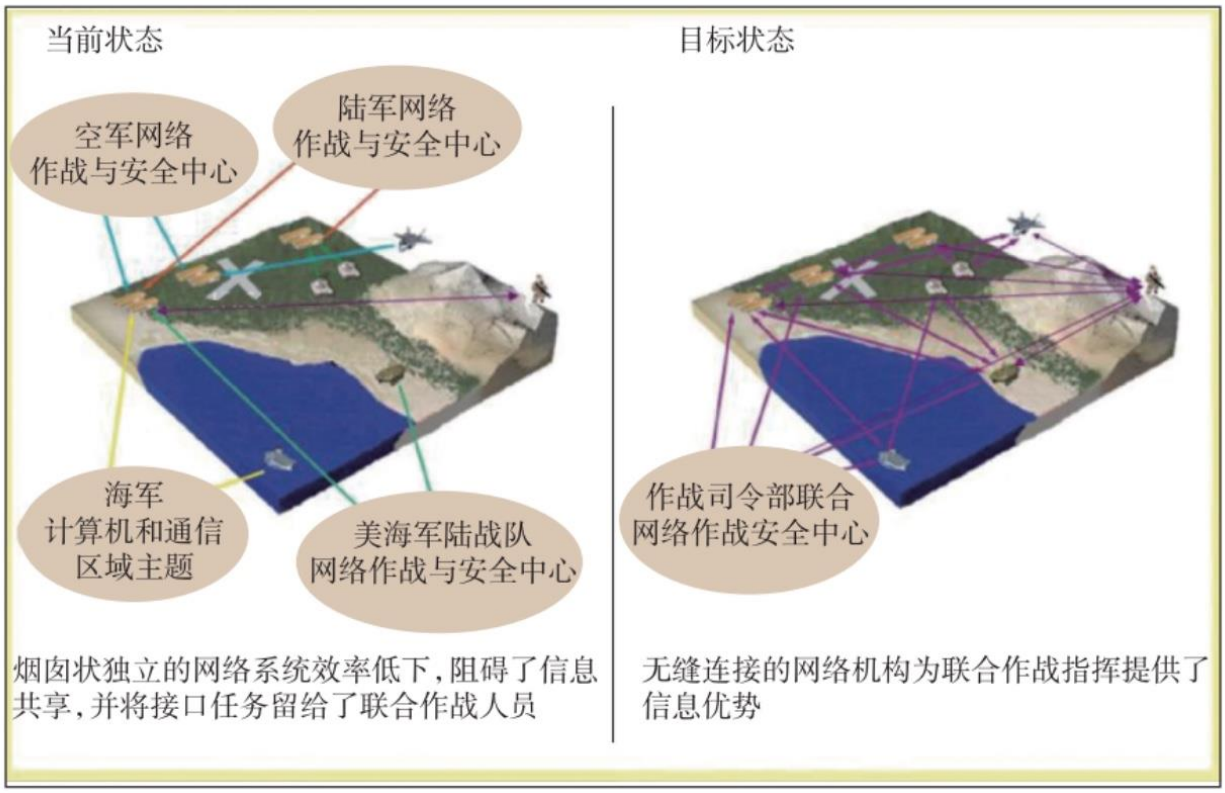
1.3.1.2 现有信息基础设施存在问题

当前，美军军事通信网络是一个覆盖全球的广域网，即“全球信息栅格”(GIG)，集成了互联网、电话、视频会议等网络功能。GIG 可以为所有军事用户提供各种保密或非保密的语音、视频与数据传输服务。随着各类完全不同、不兼容的信息技术(IT)能力的扩散，GIG 已经成为一种异常复杂、规模庞大且容易受到攻击的通信网络，经济上也承受着巨大的维持压力。

1）缺乏互操作性

通过全球信息栅格建设计划，美军在过去二十多年中已经开发了许多面向特定战场功能的作战网络与软件系统，形成了 2000 多个数据中心，但这些网络或系统的集成化程度并不高，特别是军种之间的互联互通困难，严重的妨碍了信息共享效率，而云计算等技术的逐渐成熟和应用，为美军新一轮的信息基础设施现代化提供了契机。

图 6：联合基础设施

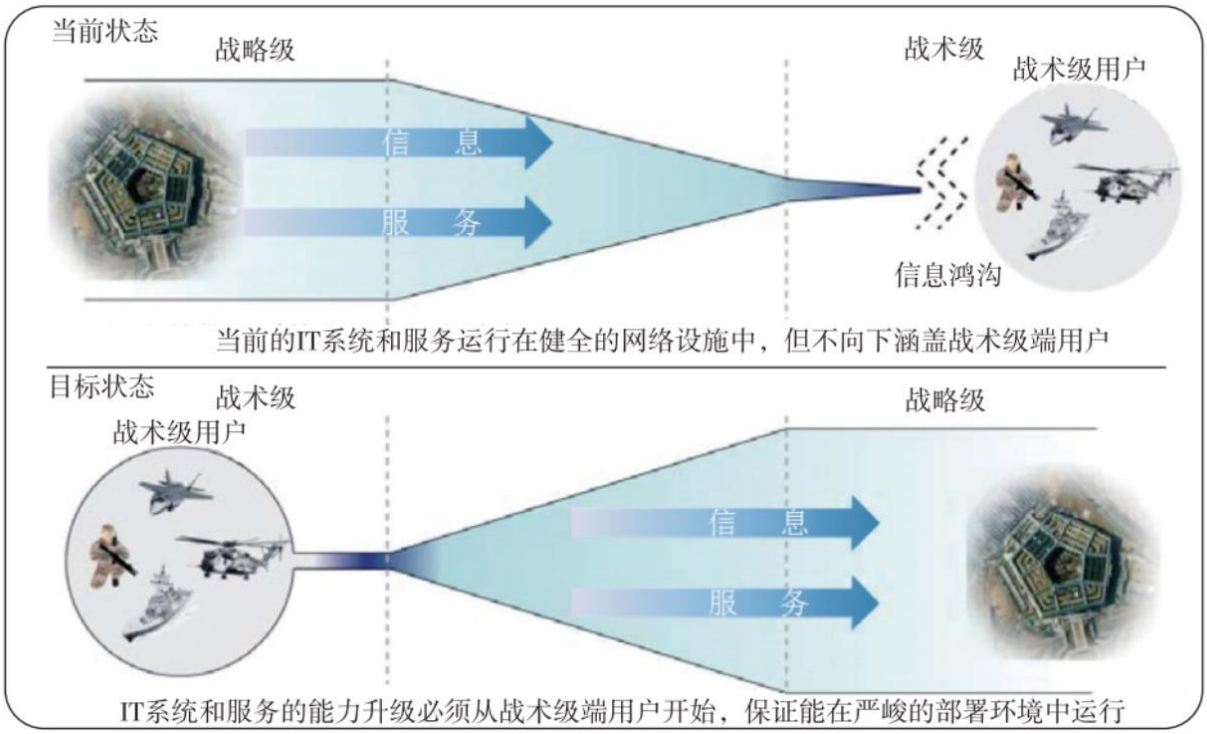


资料来源：网络资料，东兴证券研究所

2）高昂成本难以适应快速的技术变化

美国联邦政府的信息技术资产分布广且分散．维护经费大约需要 760 亿美元。然而如果能够进一步缩减 IT 管理费用、合并数据中心、去除网络冗余、对应用程序实行标准化等，那么这笔巨大开支便可以节省 30%。除此之外，在军事网络方面，那些不必要的开支也因为世界不同地区军事指挥所之间安全性、硬件和软件许可之间管理标准的差异。以及这些资产归属于不同军兵种而大量存在。如果考虑雇佣冗余 IT 员工的费用，那么这笔额外开支更大。

图 7：信息和服务边缘化

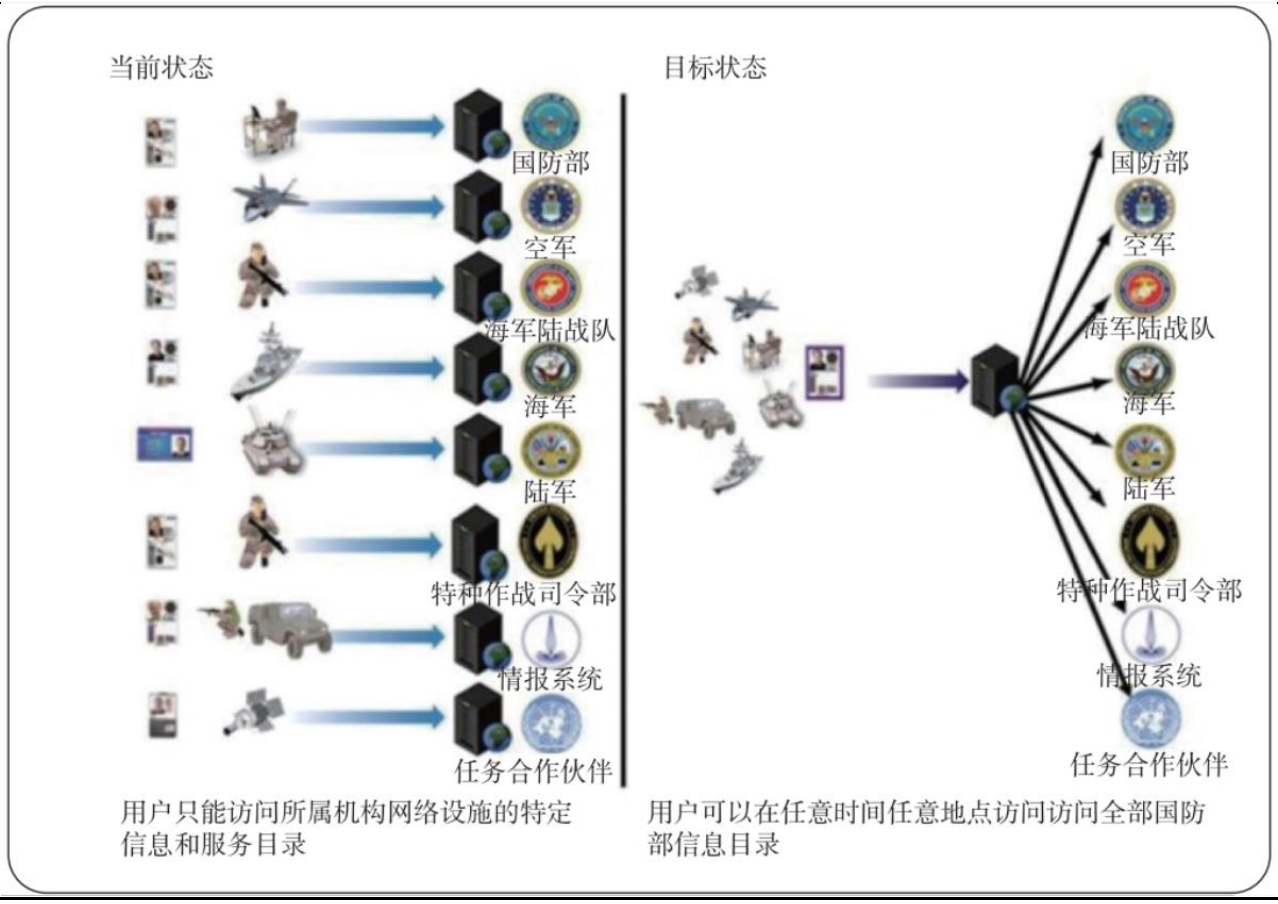


资料来源：网络资料，东兴证券研究所

3）现有系统存在信息安全漏洞

为了解决信息共享与信息安全问题、保持美国在网络空间的优势地位。必须加快美国国家网络的现代化进程，这也是美国数年以来一以贯之的重点工作。为此战略目标. 国防部也意识到军用和其他保障网络现代化的必要性。美国防部现有信息网络极度依赖 GIG，但由于 GIG 采用了网络中心的架构，本身存在严重的安全漏洞，任何对 GIG 系统或子系统的蓄意破坏都将妨碍任务执行，导致网络中心化的武器无法使用，直接影响各作战层级互信的交互数据和信息，限制按照任务指挥的要求建立和维持通信，联合部队也就无法实施全球一体化作战。因此，通过提供网络端到端的可视化，JIE 对生成决定性联合部队起到重要作用，确保战斗人员即便在面临干扰或损伤的情况下也能够获取信息。

图 8：统一的身份认证、访问控制和目录服务



资料来源：网络资料，东兴证券研究所

美军从 20 世纪 20 年代以开发半自动化防空指挥控制系统为起点，迄今已过去 90 多年，但其互联互通的综合性军事信息系统仍未完全建成。造成这种局面的原因有多方面．但最重要的一条就是各军种和相关部门各自为政搞建设，标准不统一．不能互联互通．致使近年来不得不大量拆除“烟囱”。

1.3.1.3 新的技术提供的发展机遇

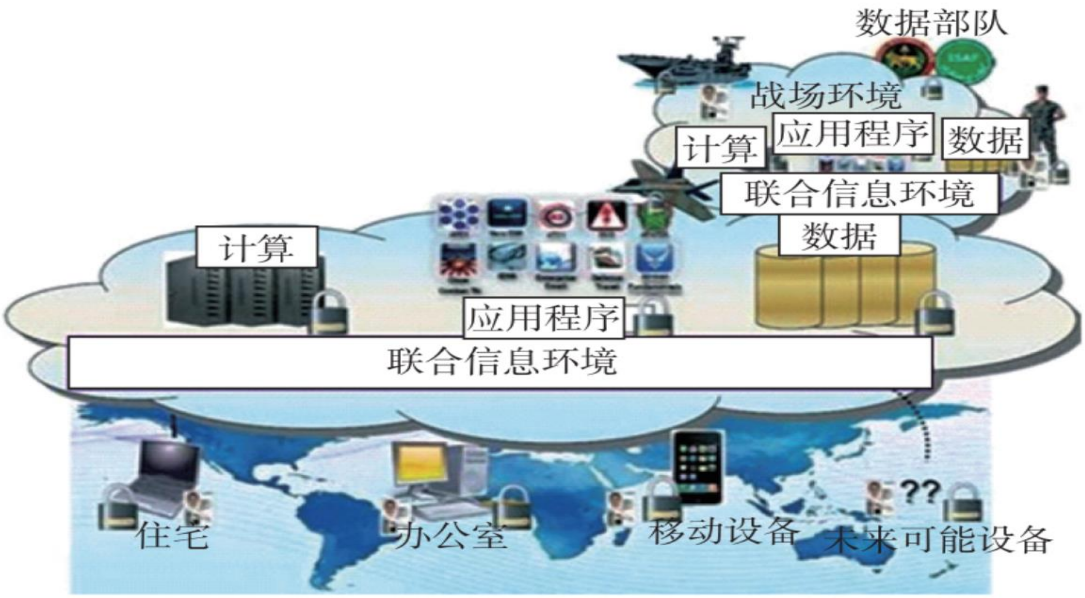
要实现全球一体化作战，必须有先进的信息技术作为保障。21 世纪以来。网络相关技术成为电子信息领域的使能力量。其中最具代表性的技术当属云计算技术、大数据、移动技术和智能终端技术。形成了完整的新一代信息技术生态系统，将国防部的网络进行高度浓缩、整合为一个共同的、全球性的、基于云的系统，以共享服务，如电子邮件、互联网接人和应用。这些技术发展为美军实施新的作战指挥方式、弥补现有国防信息基础设施不足、节约成本和提高效率提供了必要的基础性条件。特别是云计算技术，甚至有人预言，云计算将主导新信息时代的战争。“基于云计算的指挥控制技术是美军全球一体化作战的重要支柱”。

1.3.2 JIE 的核心技术及实施路线图

美国国防部面临的一个主要挑战是从传统基础设施转变到共享的基础设施，这就必须将全球信息栅格基础设施转变为一个更加充满活力和可适应的共享环境，以支持全球

网络中心行动。JIE 几乎集中了所有关键国防部信息技术的努力，并将明确提出一个陆海空三军共用的安全体系结构。

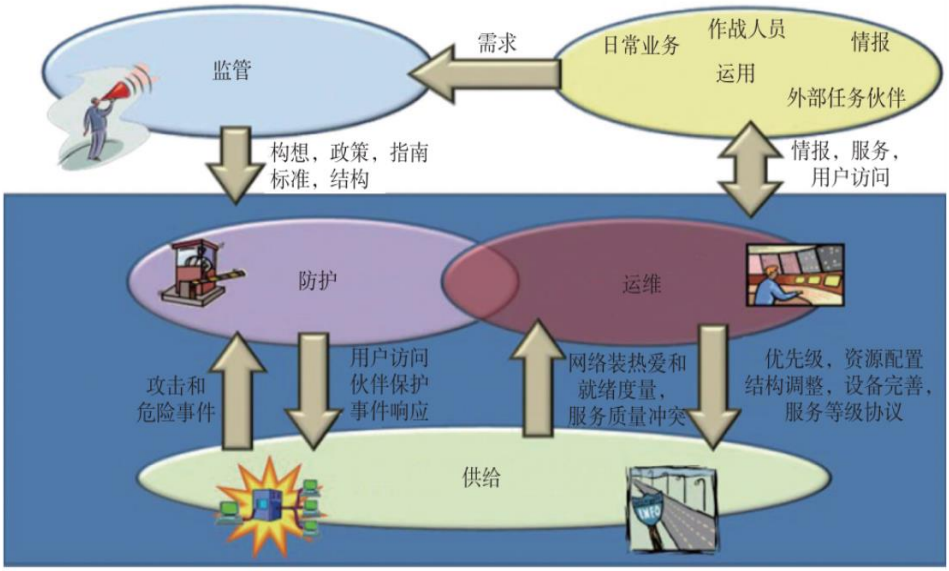
图 9：联合环境最终状态示意图



资料来源：网络资料，东兴证券研究所

JIE 按照前所未有的规模持续地进行新技术能力开发，几乎将触及美军所有组织机构。技术特点包括防御性和单一的网络——从战术到策略层面；整合国防部的数据中心和网络操作中心；以及常用的安全结构，将国防部现在这种组织中心化、网络一服务的架构改变为以实战为重点、信息中心化的架构。

图 10：信息体系联合信息环境活动模型



资料来源：网络资料，东兴证券研究所

1、单一安全架构(SSA)

单一安全架构将打破网络安全边界、降低国防部外部攻击面、更好扼制赛博攻击，提高机动反应能力，实现标准化管理、作战和技术安全控制。建设单一安全架构(SSA)的最终成果是一系列能力，使国防部赛博部队可以“看见、检查、阻止、收集”网络流量，为联合作战人员提供一个可信的信息环境。

2、网络整合

国防部现有分散的网络、处理和存储基础设施妨碍了战斗人员和任务合作伙伴之间的内部和外部合作。因此，实现 JIE 的最基础性工作就是建设一种单一、保护性信息环境，从而实现作战人员之间安全、可靠、无缝的互联互通。

3、身份与登录管理

建立强大的身份和登陆管理(IdAM)能力可以让联合作战人员和他们支持的任务领域都能够经过授权安全地获取所需的信息和服务，不受位置影响。另外，这还可以提高作战指挥员的信心，作战单位能够读取任务核心信息和服务，同时维护这些信息资产达到相应的安全性。

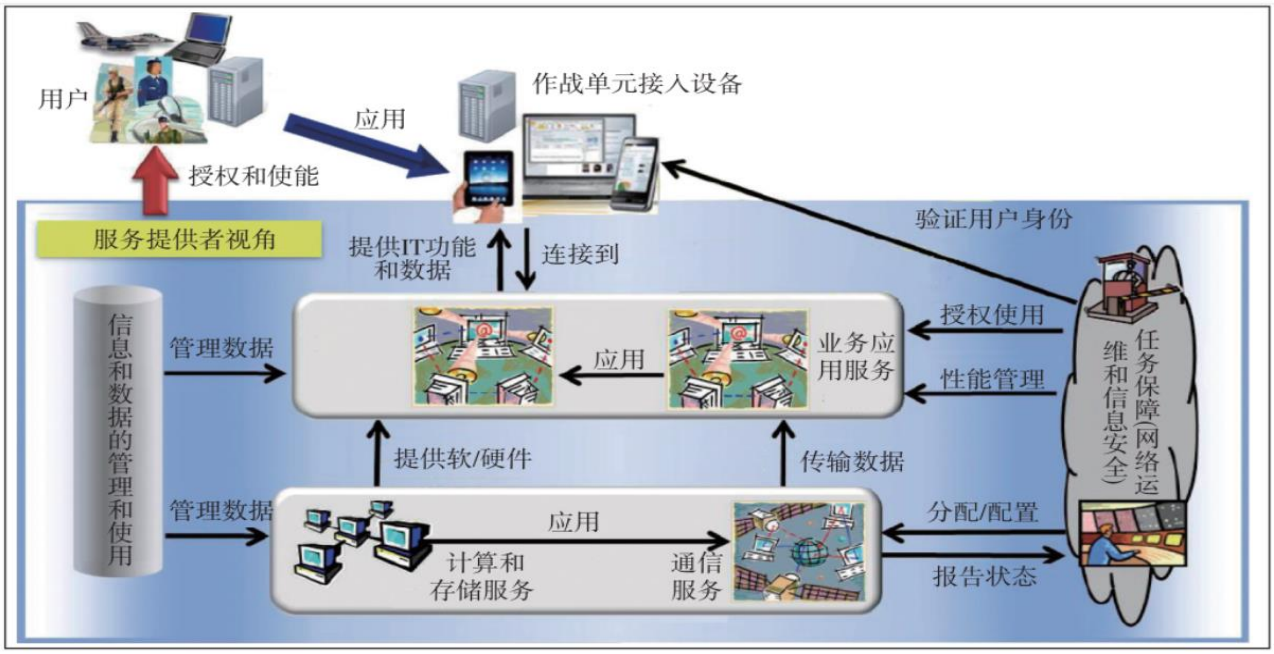
4、企业服务

企业服务是一种就像电子邮件一样的服务。在国防部内部按照通用方式、由一个单一组织作为企业服务供应商来提供。国防部一直强调将开发和部署企业服务作为 J[E 的一部分，这种服务将按照在连接断开、不连贯或低带宽(DIL)的信息环境下运行来设计，有助于保证联合作战人员和他们的任务合作伙伴发现、登陆、使用信息资产，取得任务成功。

5、云计算

最近发布的《参谋长联席会议主席(CJCS)关于联合信息环境的白皮书》将云计算技术看作联合信息环境的关键技术，“联合信息环境包括若干网络化作战中心、若干整合的核心数据中心、基于云应用程序和服务的全球身份管理系统”。“基于云计算的指挥控制技术是美军全球一体化作战的重要支柱。军事网络必须紧跟民用网络的发展步伐．加快开发用于态势感知的通用数字工具”。旧国防部向云计算转移将面临挑战，特别是成千上万台服务器、赛博安全(作为单一安全架构的部分)、抗毁性、失效备援的管理，以及软件应用程序迁移向云上迁移。

图 11：信息体系联合信息环境作战概念图

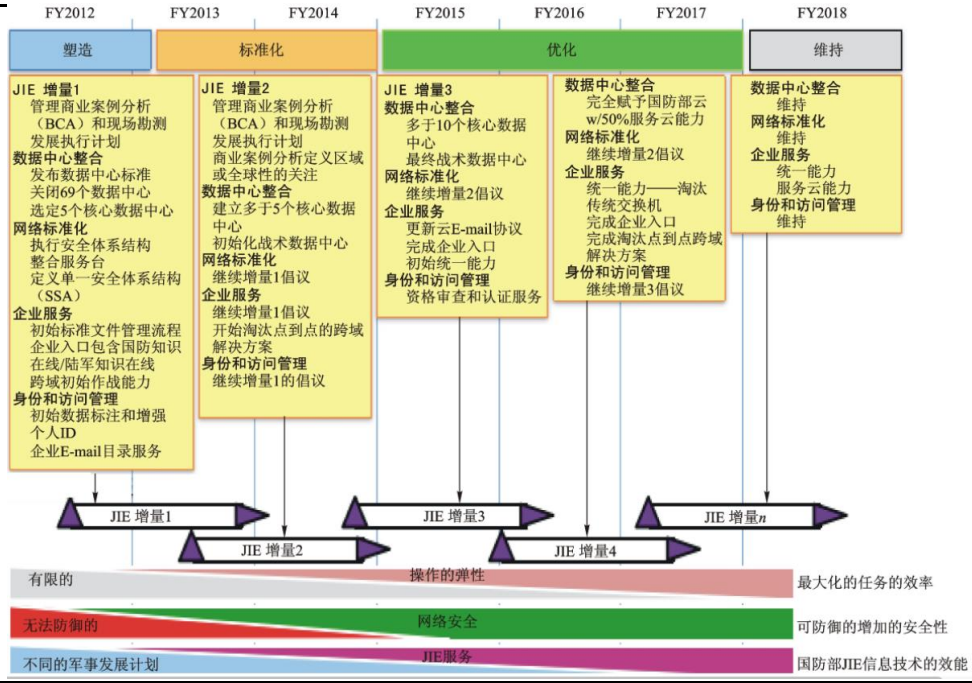


资料来源：网络资料，东兴证券研究所

6、数据中心整合

国防部将继续通过关闭并合并国防部数据中心来增强计算能力，同时确认识别能够向 JIE 核心数据中心(CDC)转移的数据中心。数据中心合并工作将有助于国防部建设一个标准化的计算架构。

图 12：JIE 发展进程



资料来源：网络资料，东兴证券研究所

1.3.3 JIE 的核心诉求

联合信息环境属于国防信息基础设施的范畴．是 GIG 的延续，建设的基本目标是为了满足美国联合作战的需要，是美国构建联合部队 2020 之路的第一个具体变化。JIE 将改变美军现有信息集成、配置、接人、共享以及技术使用方法。利用 JIE 形成的信息环境，可以在需要的时间和地点灵活地生成、存储、传播、读取数据、应用程序和其他计算服务。在发生非授权登陆时更好地保护信息的完整性，同时从整体上一以贯之地提高对安全漏洞的响应能力。

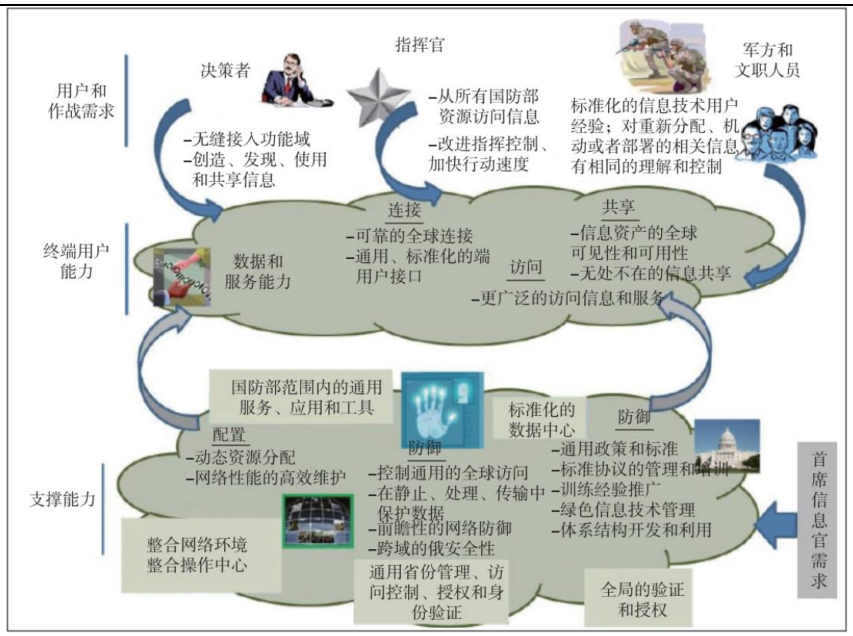
图 13：JIE 核心诉求

为指挥官优化效能	JIE 支持联合部队指挥官(JFC)的赛博行动规划； 在紧急情况下，行动所需的企业服务和服务专用应用程序确保可用； 联合部队指挥官(JFC)与任务和联盟伙伴具备安全、可靠的通信； 保证指挥官： 能够实现预期的作战效果； 能够使用需要的信息和服务； 能够在降级的 JIE 中开展行动。
对国防部 GIG 行动和防御性赛博行动的指挥控制进行优化	指挥官和支持性企业作战中心通过指导响应行动和紧急规划，对恶意赛博行动进行防护； 将复杂程度和冲突降至最低，同时保持行动的连续性和可理解性，保证任务的成功； 形成任务关键性决策，形成有效响应，适应方向变化，但不会偏离最初的任务方向。
提供 JIE 行动状态和赛博安全状态的态势感知	单一安全架构传感器状态在全球企业作战中心(GEOC)和企业作战中心(EOC)是可见的； 企业作战中心(EOC)能够检测并管理 JIE 配置变化，保证系统的健康和完整性。这些行为包括： 企业服务管理； 网络管理； 卫星通信管理； 电磁频谱管理。 在 GEOC 和 EOC 中可以看到构成 JIE 的网络、系统、应用程序、企业服务中的所有运行情况数据； 从基地、指挥所、营地和站点(B/P/C/S)向 GEOC 和 EOC 自动报告国防部信息网络配置和脆弱性状态。
优化国防部信息网络的安全性/赛博可防御性	通过单一安全架构(SSA)对 JIE 进行保护； EOC 可以有效地 通过对国防部和美国赛博司令部(USCYBERCOM)策略和预先行动路径的自动化管理，实现国防部网络的的被动防御； 通过单一安全架构(SSA)激活规则集，抗击赛博攻击，实现赛博实施的网络防御； 自动识别脆弱系统、查明配置、确定不当配置和无补丁系统中的运行风险； 迅速对网络进行重新配置，阻止高级持久赛博威胁，确保任务的完整性和连续性。

资料来源：网络资料，东兴证券研究所

JIE 的最终受益者将是战术级战地指挥官和部队，它可以更好地对信息技术、战斗和网络安全快速集成，满足当前快速变动的条件要求。利用 JIE 传送的作战能力让指挥员可以将指挥艺术与控制科学完美结合。让联合部队 2020 按照要求灵活地集成作战功能、应对不断出现的军事挑战。

图 14：信息体系联合信息环境能力视图

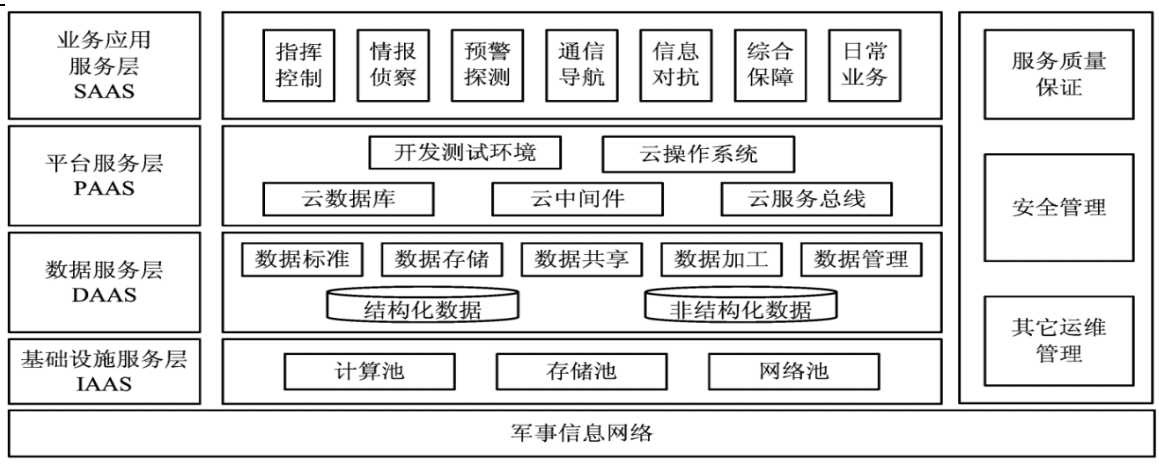


资料来源：网络资料，东兴证券研究所

2. 军事云到底是什么？

军事云计算，简称军事云，就是应用云计算的关键技术，建设军事数据中心等硬件基础设施体系，开发军事领域相关应用服务等软件体系，依托军事信息网络，向军队的单位或个人用户提供云计算服务。

图 15：军事云计算的体系框架



资料来源：网络资料，东兴证券研究所

军事云计算不同于民用云计算的特点为：军事云计算工作在复杂电磁环境和强网络对抗的环境之下，对于信息安全保密具有极高的要求，主要应用目标服务于军事效能和战斗力的提升。

2.1 云计算在美军中的应用

美国国防部国防信息系统局从 2008 年就开始研发云计算解决方案，主要包括 Forge．mil、RACE(Rapid Access Computing Environment，快速响应计算环境)和 GCDS(GIG Content DeliveryService，全球信息栅格内容传送服务)。

经过长期的建设，美国国防部信息系统成为了全球最大的异构、分布式复杂系统，存在系统脆弱、维护困难、效率低、能耗大、互操作性不强等问题。 为此，2012 年，美军提出了联合信息环境 （ Joint Information Environment， JIE）建设计划，将按照“标准化” 和“体系化”的思路，建设一体化、安全、高效的信息体联合信息环境。

为了指导、规划联合信息环境的建设，统一各类人员对网络中心作战能力建设的认识，美国国防部首席信息官办公室在 2012 年 7 月发布了国防部信息体体系架构（DoD Information Enterprise Architecture，DoD IEA）。 IEA 运用国防部体系结构框架 2.0（DoDAF 2.0）方法，构建了 13 个体系结构产品，描述了联合信息环境（Joint Information Environment，JIE）的构想、使命任务、活动、功能、能力等，为从事作战指挥、规划计划、建设管理、系统设计、技术研发和系统维护等各类人员提供了统一规范的描述。

在全球范围内，美军将云计算作为军事领域一项极具发展潜力的技术，研究将其应用到军事信息系统中的方法。

美军各部门自 2008 年开始，就已与 IBM、惠普等 IT 公司合作，研发了多个军事云计算项目，其中典型的如下表所示。美军不仅打算利用云计算良好的经济性，以削减其庞大的信息技术军费开支，更是做好了在战场上使用云计算系统的准备。其中全球信息栅格内容分发服务(GCDS) 已在阿富汗战场上投入使用，在协同、共享信息以及分发信息的过程中发挥了重要作用。

2012 年，美国国防部在美国联邦云计算战略的基础上，结合美军在军事云计算领域的实践，发布了国防部云计算战略。国防信息系统局云计算的发展计划已经取得了重大进展，正在逐步建立和完善云计算的基础设施、协同软件平台以及相关网络服务。

表 1：美军现有的军事云计算项目

军事云计算项目	部署部门	服务类型
全球信息栅格内容分发服务(GCDS)	国防信息系统局	基础设施即服务
快速访问计算环境(RACE)	国防信息系统局	平台即服务
Forge. mil 开发平台工具	国防信息系统局	平台即服务
在线联合防御(DCO)	国防信息系统局	软件即服务
人事服务交付改革(PSDT)	空军	软件即服务
海军私有安全云	海军	软件即服务
企业电子邮件	国防信息系统局/陆军	软件即服务
陆军体验中心(AEC)	陆军	软件即服务

资料来源：网络资料，东兴证券研究所

随着联合信息环境（JIE）已经进入 2018 阶段，当前美军对于新型技术如云计算、人工智能、大数据等投入愈发加大，三个领域的军费预算已经从 5 年前的 56 亿美元增加到 2016 年的 74 亿美元，2018 年九月美国国防部高级研究项目局宣布，投资 20 亿美元开发下一代人工智能技术，预计未来会继续增加。

2.2 美军青睐 AWS 的云计算能力

目前美国防部的用户包括：140 万现役人员；78 万美国本土雇员，120 万国家安防和预备役人员；550 万以上的家庭成员和部队退休人员；分布在超过 146 个国家、5000 个以上的办公地点，60 万栋以上的建筑。各种 IT 系统包括：超过 1 万种系统（其中 20%的系统和关键任务相关）;约 1850 个数据中心;约 65000 台服务器;7000 万台以上的计算机和 IT 设备；数以千计的网络；数千台邮件服务器、防火墙、代理服务器等；移动设备包括 49.3 万黑莓手机、4.1 部苹果设备，8700 部安卓设备等。

国防部现在拥有大约 500 个不同的云计划,在云基础架构商业解决方案上有很大需求。美国国防数字服务部门(DDS)表示，在云技术方面，军方严重落后于私营企业。

国防部副部长埃伦·洛德谈及云计算：“我们必须接受改变，如果我们利用商用云解决方案，我们将拥有基础技术，我们需要更快地为我们的作战人员提供更好的软件，更好的安全性和更低的成本，并且软件将更容易维护，如果我们继续以同样的方式开展业务，我们的软件将过时，其成本将远远超过其需求，我们将无法吸引最优秀的软件人才，我们将失去技术优势。改变是不舒服的，但正如我一直告诉我们的团队，我们需要感到不舒服。”

AWS 是目前美国政府批准处理秘密和绝密数据的唯一公司。作为中央情报局 6 亿美元内部部署云的承包商，亚马逊在托管机密数据方面远远领先于其他行业。

2018 年 2 月，美国国防部曾把一份 9.5 亿美元的合同给了亚马逊的合作伙伴 REAN Cloud，用于将信息系统迁移至云端，此举在业界引发轩然大波，甚至遭到甲骨文公司起诉，后来五角大楼不得不发表声明称，该决定是由五角大楼在硅谷设置的创新部门所做的，并随机把合同金额缩水至 6500 万美元，合同涉及范围也大大缩小。

EDI，即五角大楼的联合企业防御基础设施云计算解决方案合同。该合同要求一家公司帮助五角大楼在更广泛的范围内使用云计算，构建一个安全的信息环境，跨越国内战术的全球战术优势，并能迅速获得计算和存储能力，以应对作战挑战。据了解，该合同在 10 年期间的价值可高达 100 亿美元。

2018 年 7 月 26 日，在近两个月的推迟之后，五角大楼终于对联合企业防御基础设施（JEDI）合同展开竞标，在最终的征求建议书（RFP）中明确表示，国防部将会为这份价值 100 亿美元的云计算合同选择一家提供商，也就是说这是一份为期 10 年的“赢者通吃”的合同。早期，科技公司有望组成联盟共同为五角大楼提供云服务，但从 REP 的最终版来看，五角大楼还是决定押注在一家公司身上。虽然 RFP 中明确表示，竞标是公开透明的，没有谁有特权，但是亚马逊 AWS 仍然因领先的云计算能力和与 CIA(美国中央情报局)的人工智能合作被认为是胜算最高的选手。

RFP 中明确提出了公司必须满足的「硬性标准」——中标公司在授予合同后 6 个月内托管机密数据，并在 9 个月内托管绝密/敏感分区信息。就目前来看，AWS 是唯一能够满足这一标准的云服务提供商。

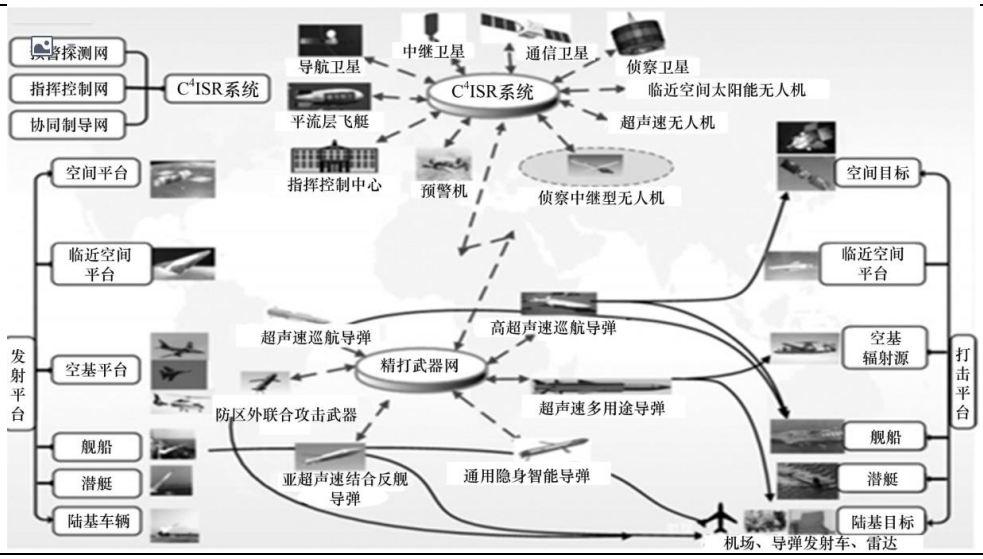
云计算确实是赢家通吃的行业，即使在军工领域仍然有效，AWS 有望凭借超群的技术优势，未来取得更多的军方订单。

2.3 美军构想的信息战争样式

网络中心战是信息时代的战争样式，是以网络技术为核心，以信息共享为基础建立信息优势，利用信息优势实现决策优势，从而加快决策和指挥速度，实现作战协同，提高杀伤能力、生存能力、响应能力以及自我协调能力， 以极大提高作战效能。

网络中心战的实质是利用网络实现所有作战要素信息共享，达到实时掌握战场态势，缩短决策时间，提高打击速度与精度的目的。具体体现：通过稳定可靠的网络化能力提升信息的共享程度；通过信息共享来提高信息质量和战场态势感知共享能力；通过战场态势感知共享来促进协同和自我协调能力，提高持续作战能力和决策速度。是一种集侦查、情报、计算、监控、通信、指挥控制、杀伤于一体的 C4KISR 系统间的对抗。

图 16：美军构想的信息战争样式



资料来源：网络资料，东兴证券研究所

对于网络中心战的进一步发展，是整合陆、海、空、天、赛博等多维作战力量，各传感器、作战平台、武器系统组成虚拟存在的“云”，在体系层面实现战场资源的动态高效管控、海量异构信息实时、高速、分布式处理共享，构建跨领域、跨军种、分布式、网络化的“云杀伤”协同作战云。

表 2：美军近期开展的动态与分布式作战项目列表

典型项目	时间	主导机构	能力/性能	作用/目的
UFP 可升降有效载荷及九头蛇无人母艇	2013 年	DARPA	载荷存储与发射	水下战区部署、长期值守、即时唤醒、快速发射载荷作战概念； 试验远距离水下相关通信技术； 多种载荷装载能力等。
SoSITE 系统之系统作战系统项目	2014 年	DARPA	系统架构	系统级架构，如电子模块载荷的开放接口标准，综合射频相关标准等； 系统之系统级架构，SoSITE 项目研究的重点，包括各种系统之间的开放系统接口标准 OSA 等。
CODE 协同作战项目	2014 年	DARPA	平台认知、协同能力	发展新型软件和算法，提高现有无人机在高对抗环境中的任执行和协同作战能力。
STRATUS 项目、DBM 项目	2014 年	MBDA、DARPA	作战管理、决策辅助	开发用于作战管理的控制算法和决策辅助软件、用于驾驶舱的先进人机交互技术，形成管理空空、空地作战任务的综合分布式管理能力。
Gremlins 项目、LOCUST 项目	2015 年	DARPA	无人平台空中部署、重复使用	通过在防区外发射携带有侦察或电子战载荷、具备组网与协同功能的无人机“蜂群”用于 ISR、电子攻击，并在任务完成后对幸存无人机进行回收。

资料来源：网络资料，东兴证券研究所

作战云是基于网络化的信息基础设施，采用面向服务的模式，为指挥决策、部队行动、武器打击提供按需、便捷、快速的专业、权威的数据和应用服务，与民用的“云“相比较，作战云的特点主要表现在以下 3 方面：

1）信息系统的组织性、计划性的要求更高；

2）在严酷的环境中可靠性和安全性的要求更高；

3）信息服务的正确性、精确性、实时性、专业化的要求更高；

协同作战云作为未来军事作战的核心，其要求是反应快速、决策正确、反馈及时。

美军全球指挥控制系统可连接全球 100 多个作战基地与冲突热点。美军参谋长联席会议通过该系统，只需 40s 就可与国外 11 个联合司令部和特种司令部联络。借助于该系统，美总统向前线部队下达命令仅需要 3min～6min，向核部队下达命令也只需要 1min～3min。

2.4 军事信息系统发展对云计算的需求

2.4.1 进一步加强军队信息化建设和军事信息资源集中统管的需要

随着军队信息化建设的快速发展， 各部门因为自身业务的需要建立了大量军事信息系统的“烟囱”。这些军事信息系统在建立之初都发挥了其应有的作用，但因为在顶层设计时缺少统一整体的规划， 导致现阶段面临一体化联合作战信息互联互通的需要时，“烟囱”之间出现数据共享困难的问题。在指挥信息系统方面， 虽然可以通过系统综合集成的方法解决信息系统之间的“烟囱”问题， 但这种方法属于对已有系统的集成改造， 具有一定的局限性。

解决这一问题的根本方法是在新的军事信息系统构建之前即加强对军队信息化建设和军事信息资源的集中统管， 做好顶层设计和整体规划。通过利用云计算技术统一的服务平台和面向服务的体系架构，对现有的军事数据中心软硬件进行合理的整合，构建全军统一的军事信息基础设施平台，实现信息资源全军共享，并提升系统互联、互通和互操作能力， 从而有效解决军事信息系统“烟囱”林立的问题， 满足军队信息化建设和军事信息资源集中统管的需要。

2.4.2 战场环境下对高性能计算和移动计算能力的需要

在未来信息化战场环境下，大量传感器的部署、一体化联合作战指挥信息系统和军用物联网的运用等都将产生大量的实时数据，对这些战场大数据的高效处理，关系到指战员信息优势和决策优势的获取。现有指挥信息系统的架构满足不了战场环境下高效信息处理的需要，而云计算架构强大的计算能力却可以很好地解决这一问题。另外，军用智能手机、平板设备等瘦客户端因为其便携灵活的特性，可以更好地适应未来信息化战场遂行机动、信息快速获取和分发的需要。对这些移动信息终端进行战场信息保障，从而满足其移动计算和随时按需计算的需要，也有赖于战场军事云的部署与支持。

2.4.3 增强军事信息系统安全防护能力的需要

军事信息系统工作于复杂电磁环境和高强度网络对抗环境之下，战时还面临着敌方硬摧毁的威胁。这些都导致信息融合共享与安全保密成为不可调和的矛盾，严重影响了军事信息系统使用效益的发挥。为此，保证信息安全共享就成为军事信息系统建设的一个重要目标。

首先，对于军事信息系统面临的网络威胁，可以借鉴云安全和安全服务的概念，综合利用现有的安全技术，构建基于云计算的统一的网络防御架构，以增强军事信息系统网络安全防护能力。其次，对于敌方硬摧毁的威胁，云计算架构逻辑上集中、物理上

分散的分布式的特点可以保证军事信息系统具有较强的抗毁性和生存能力，云数据中心良好的灾难备份与应急响应的特性也可以有效增强军事信息系统的鲁棒性。

2.5 军事云的具体应用设想

对于军事云在军事信息系统中具体的应用领域，可以作出以下设想:

一是在日常办公业务信息系统中，包含军事训练和培训、人力资源管理、办公自动化等，提供全军统一的信息服务。除过机密数据的存储与处理，完全适合使用云计算架构。

二是在情报信息处理领域，包括侦察监视情报、预警探测、模拟仿真等产生的大数据，需要借助云计算进行数据的存储、处理、共享和融合。

三 是在战场信息保障方面，构建战场“作战云”，借助更简捷的移动指挥平台，实现联合作战部队自主协同、透明的战场环境、科学的作战决策等多方面信息支持。

四是在军事信息网络安全防御方面，借助云计算架构，增强军事信息网络安全的态势感知能力，并且通过基于云计算的统一的网络主动防御架构，将安全作为一种服务提供给军事云用户。

五是在军用物联网领域，将云计算架构作为军用物联网的信息处理核心，在物资管理、战场救护、后勤保障和装备保障信息支持方面发挥重要作用。

3. 安全，是云计算在军事领域应用的第一要务

美国五角大楼出于信息安全考量，决定由 Windows 逐步转入以 Linux 为基础的操作系统。俄罗斯国防部将所有办公电脑使用的微软正版 Windows 视窗操作系统改为国产的 Astra Linux，成为俄军唯一操作指挥系统。Astra Linux 操作系统自带办公应用软件，并使用“黄蜡纸”电子文件流通系统进行加密的信息传输，具有独一无二的信息保护功能。由此可见，网络安全战上升为国家战略范畴，其安全防泄密将是重中之重。

网络空间安全的提出背景是基于全球五大空间的新认知，网络领域与现实空间中的陆域、海域、空域、太空一起，共同形成了人类自然与社会以及国家的公共领域空间，具有全球空间的性质。有学者提出这样的观点:“网络空间安全”是指能够容纳信息处理的网络空间构建与管理的安全，是远比“信息安全”更为重要和根本的安全。

3.1 军事信息网络安全面临的几大威胁

网络安全从其本质上来说是网络的计算机上的信息安全，是指计算机系统的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改、显露，确保系统能连续正常运行。军事信息网络安全威胁主要有以下几点。

1）计算机病毒

现代病毒无论是传播性、隐藏性还是破坏性，都是传统病毒无法比拟的。可借助文件、

邮件、网页、局域网中的任何一种方式进行传播，具有自启动功能，并常常潜入系统核心与内存，为所欲为；利用控制的计算机为平台，对整个网络进行大肆攻击。病毒一旦发作，能冲击内存、影响性能、修改数据或删除文件。一些病毒甚至能擦除硬盘或使硬盘不可访问。

2） 网络“黑客”

这是军事信息网络所面临的最大威胁。此类攻击又可以分为两种：一种是网络攻击，黑客以各种方式有选择地破坏对方信息的有效性和完整性；另一种是网络侦察，是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得对方重要的机密信息。

3）人为因素造成的威胁

由于计算机网络是一个巨大的人机系统，除了技术因素之外，还必须考虑人的安全保密因素。如国外的情报机构的渗透和攻击；内部人员的失误以及攻击。表现在敌对者可能会采取打进来，拉出去的方法，利用系统值班人员和掌握核心技术秘密的人员，对系统安全进行攻击等。

4）实体摧毁

实体摧毁是计算机网络安全面对的“硬杀伤”威胁。主要有电磁攻击、兵力破坏和火力打击三种。

3.1 美军网络空间安全战略主要内容

从美军发布的一系列涉及到网络安全战略的文件和美军在网络战方面的建设来看，美军网络空间安全战略主要内容包括 5 个方面：

（一）网络空间军事化战略

2003 年 2 月发布的《确保网络空间安全国家战略》，把网络空间安全提升到与国家经济安全和军事安全同等重要的位置，提出了美国网络空间安全三大战略目标：阻止对美国关键基础设施的网络攻击；降低国家面对网络攻击的脆弱性；如果网络攻击发生，最大限度地减少损失和缩短恢复时间。

2011 年 7 月发布的《网络空间行动战略》，为美军提供具体的网络空间行动指南，将网络空间列为与陆、海、空、天并列的行动领域，国防部以此为基础进行组织、培训和装备，从而确保在网络空间采取军事行动的能力。美国防部多年前就开始着手打造一支技术先进的网络战部队。2009 年 6 月，专门成立了网络司令部（Cyber Command），负责计划、协调、组织和实施各类网络空间作战行动，包括指导国防部信息网络的防御行动，准备和实施网络空间的攻击行动，确保美军及其盟国在网络空间的行动自由，剥夺敌人在网络空间的行动自由；随后还颁布了相应的网络空间作战条令。美国陆海空三军都有相应的网络司令部和网络战部队，包括陆军网络司令部、海军网络司令部/第 10 舰队、空军第 24 航空队、海军陆战队网络司令部和海岸警卫队网络司令部。目前，美军共有 3000～5000 名网络战专家，5～7 万名士兵涉足网络战；加上原有的电子战人员，美军的网络战部队人数在 8.8 万人左右，相当于 7 个 101 空降师；其

中，空军网络战力量最强，共有 2.5 万人。

二）网络空间积极防御和威慑战略

美军传统的网络安全防御主要依据其提出的“信息安全保障”（IA）思想，即确保网络中信息的保密性、完整性、可用性、可控性和不可否认性，并通过防护、检测、反应能力来实现网络系统的可恢复性；同时美军还提出了“纵深防御战略”，认为信息安全保障要依靠人、技术和操作（行动）来实现包括网络基础设施防御、网络边界防御、计算环境防御和支撑基础设施防御等目标。

2011 年 5 月发布的《网络空间国际战略》，宣称美国将使用一切必要手段防御网络资产，像对待其它任何威胁一样，对网络空间的敌对行为作出回击，并保留诉诸武力的权利。为了更加有效地阻止、击败针对美军网络系统的入侵和破坏行为，同年 7 月发布的《网络空间行动战略》，提出“变被动防御为主动防御，从而更加有效地阻止、击败针对美军网络系统的入侵和其他敌对行为”的“积极防御”战略措施，通过各种手段发现、监测、分析并减轻网络面临的安全威胁和存在的安全脆弱性，在“有害代码造成损害之前”就“侦测”并“阻止”它，即在网络尚未遭到攻击前阻止恶意行为。

“转守为攻”的同时，美军进一步提出了“网络威慑战略”，即在不削弱进攻能力的前提下，拥有对方难以承受的报复和摧毁能力；要明确告诉敌方，他们要为其网络攻击行为付出代价。公开宣称，网络司令部有权对境外计算机发动“先发制人的行动”、甚至“用炸弹回击黑客袭击”。最极端的情况是，在对其他国家采取常规军事打击行动之前，可首先通过网络攻击瘫痪敌方网络系统，从而使得敌方无法通过攻击美军指挥控制系统及美国关键基础设施，来阻滞美国的军事行动。

（三）网络空间安全国内合作战略

《网络空间行动战略》表明美国国防部试图建立美国国内的联盟，加强美国防部与国土安全部等其他政府部门及私人部门的合作，在保护军事网络安全的同时，加强电网、运输系统等重要基础设施的网络安全防护，构建全民防御体系。安全战略强调国防部要与国土安全局等部门建立分工合作协调机制，要与从事关键基础设施软硬件生产的公司进行合作，如共享网络安全态势信息，联合采用安全保护措施，处置重大网络安全事件。

为加强对国防工业公司网络的保护，美国防部于 2007 年就启动了“国防工业公司网络与信息安全保障”计划。安全战略特别强调指出，由于大量软硬件产品生产过程中存在广泛的“外包”行为，“外包”厂商的安全资质，将构成重要的关注对象。显然今后从事相关生产的企业，无论是美国企业还是非美国企业，都要以某种方式受到国防部的监管。

（四）网络空间安全国际合作战略

《网络空间国际战略》提出了网络空间国际战略的 7 个重点政策：在经济领域确立国际标准，保护知识产权，建立具有创新性和自由、开放的网络市场；在网络安全领域增进合作，确保互联网安全性、可靠性和灵活性；在执法领域加强网络立法和执行力

度，提高全球打击网络犯罪的能力；在军事领域与盟友通力合作，应对网络空间所面对的威胁；在互联网管理方面维护全球网络系统（包括域名系统的）稳定和安全；在国际发展领域援助合作伙伴，建立更强更可靠的“数字基础设施”；在网络自由方面加强隐私保护，促进网络言论自由、集会自由、结社自由和信息自由流动。《网络空间行动战略》也强调“加强与美国的盟友及伙伴在网络空间领域的国际合作” 。

美军认为，网络空间是一个连接各种网络的大网络，任何单个国家或组织仅凭一己之力，都无法进行有效地网络空间安全防御。通过开展与美国的盟友及伙伴在网络空间领域的国际合作，可确保美国等西方国家在全球网络空间的话语权与掌控力，及时共享网络安全威胁信息、网络攻击事件特征和参数，提高美国及其盟友的网络空间安全态势感知警和集体防御能力。

美国国防部与盟国及其他国际合作伙伴的关系，为未来美国国际安全合作提供了坚实基础。连续的国际合作、集体防御以及国际网络空间准则的建立，将强化网络空间安全，并使各个国家受益。

但这一战略，对其他国家，尤其是那些因为各种原因注定无法被当作美国“盟友”的国家，提出了直接而尖锐的挑战：如何看待全球网络空间，如何看待美国公司提供的信息服务与软件产品，美国国防部认为“外包”到其他国家的软硬件产品可能对美国国家安全构成潜在威胁，那么同样的，由美国公司生产的网络产品是否构成对其他国家安全的潜在损害？

（五）网络空间人才和技术创新战略

《网络空间行动战略》提出网络空间行动的第五个战略措施就是“重视高科技人才队伍建设并提升技术创新能力”。美军认为，保卫美国在网络空间领域的国家安全利益依赖于美国人民的聪明才智和技术创新性。应通过实施有效的人员招募、继续教育和培训计划，建立和维持一支高素质的网络空间人才队伍。如国防部应简化网络空间人才招募流程，允许网络空间人才在国防部和其它公共机构及私人企业之间不受限制地自由流动，吸引网络空间人才为国防部服务。安全战略还强调，今后将加大对新技术的研发力度与投入，积极发展新的网络技术，并鼓励创新性研究，时刻保持美国在网络技术上的优势。如加强对“云计算”、“虚拟化”等前沿网络技术的投资，运用一些传感器和态势感知软件，提高对安全威胁和漏洞的识别能力，及早发现敌对网络中是否存在潜在的恶意代码；建设“国家网络靶场”，提供网络空间作战真实演练环境，试验和检验新的网络空间作战技术、方法和手段。

3.2 国内存在问题

对我国网络空间安全担忧乃至于对军事网络空间安全的担忧主要是因为我国缺乏自主核心技术的支撑，信息技术领域中重要的产品都是外国生产的，比如芯片、操作系统以及数据库。 没有掌握到这些技术的核心完全依赖于进口，从某些角度分析，我国的网络空间安全很大程度上受制于美国。

这一现象的主要原因有以下两点：

第一，我国的信息化进程时间段，各种信息技术和理论还不够完善，网络安全核心技术创新及研发能力不够，网络人才培养招募重视程度低，在此之前国家对信息化的重视程度不够，阻碍了我国互联网技术的进步，这也是我国大型网站频繁遭受到病毒侵袭、黑客攻击，政要人物被外界监视的原因；

第二，中国经济起步较晚，网络空间战略意识淡薄，2014 年才正式成立信息化小组，并且许多战略部署都是参考国外建设的，没有形成一套独立的、成熟的、属于我们自己的网络空间治理的指导性文件。

但国内以阿里云为代表的云计算厂商的快速崛起为我国解决当前网络安全短板提供了契机。国外 IT 八大金刚进入中国后渗透到各个领域，深度渗透至电信、金融、石油等关键网络基础设施。其中，思科公司占据了中国联通 169 骨干网约 81%、金融业 70%以及电视传媒行业 80%以上的份额，使中国经济命脉被掌握，系统运行被控制，甚至存在被依令破坏的巨大隐忧。军队中情况也非常不乐观。但随着 IT 技术的进步，IT 基础设施方面未来将被云计算所占据，八大金刚的技术优势乃至布局优势将不复存在，中国在云计算发展态势中已经在第一梯队，不存在技术代差，某些领域甚至领先。而且阿里云的云计算技术方案并不是使用 Openstack 等开源技术实现，而是通过自身团队进行了底层技术开发，自主可控能力空前提高。所以我们认为，未来国内关键领域中使用国产 IT 巨头产品的比例将逐渐提升，不再像以前存在效率和安全的权衡问题，尤其是对安全高度敏感的军事领域的 IT 基础设施建设。

3.3 我国军用网络安全技术发展现状

军用网络安全技术的发展与军事需求密切相关，一般来讲，由于军用网络承载的业务大多为各类指挥信息，涉密度高，因而对网络安全技术提出了很高的要求。但随着 IT 技术已经进入云计算时代，在当前的网络安全手段之上，仍然需要新型信息安全技术来面临新的云计算安全方面的威胁。

3.3.1 信道加密技术

军用网络干线信道主要以光纤为主，在实施机动作战时，各部队通过微波中继建立干线信道。在指挥所内部，主要是通过以太网和无线局域网建立网络连接。在战术级别，战术电台构成无线互联网。由于军用网络上传输的信息涉密度高、时间要求快，因此对信道加密技术而言，必须发展大容量、低时延的透明加密技术，通过硬件对网络数据流进行快速加密，尽量避免带宽损耗，提高通信效率。

3.3.2 网络隔离技术

网络隔离技术从整体上可以分为逻辑隔离和物理隔离两大类。军用网络大多采用物理隔离方法，其含义是公共网络和专网在网络物理连线上是完全隔离的，且没有任何公用的存储信息。但是，由于现代军事网络一般涉及有线网络、无线网络、卫星网络、数据链网络等多种网络类型，采用物理隔离时，将会导致在各个网系间交换数据十分困难，无法实现实时共享。因而，军用网络隔离技术必须解决网系融合的问题，按安全等级对网络权限进行限定，采用协议剥离、单向传输等技术确保数据交换安全。

3.3.3 身份认证技术

军用网络必须对用户身份进行准确识别，才能保证各级用户按照规定的权限存取数据，不发生越权访问事件。身份认证一般采用口令认证、生物特征认证、机器码认证等手段实施，美军为其军事人员配发了身份认证卡，确保其在任何位置、任何时间访问军用网络时，都能准确标示其身份信息。

3.3.4 终端管理技术

终端管理是对军用网络硬件资源的监控技术，通过进程管理、端口监控、驱动监视、文件访问监视等技术，确保各级终端仅能执行权限规定范围内的动作，一旦发生违规操作，将会产生报警并锁闭终端，防止事态扩大。

3.3.5 容灾备份技术

军队网络容灾备份技术目前仅能支持小规模的应急响应需求，无法满足大规模数据损毁、网络瘫痪时的应急响应要求。还没有建立容灾备份的法规制度，大规模网络的协同预警定位与隔离技术研发还处于起步阶段。

3.4 加强国产化和构建面向云计算的新型安全技术是有效的应对策略

1）加速推进军用网络国产化进程

目前军用网络软硬件系统国产化程度还不够高，主要的服务器系统、核心交换机、终端的操作系统和数据库软件，大多数采用国外产品。特别是在设计开发各类指挥信息系统时，大多数基于微软的开发平台，使得我军指控系统基本上已经“微软化”。因此，要立足于国有 CPU 和操作系统，采用国产数据库系统来构建军用网络系统，确保核心网络设备国产化，从而形成自主防护的安全盾牌，确保网络安全。选择重点领域和关键技术，确定有限目标和发展方向，如高速网络安全技术、无线网络及无线接入安全技术，下一代互联网安全技术等，有针对性地进行跟踪研究和系统研发，确保我军在建设新型网络的同时，高起点地同步进行网络安全系统的建设。

2）构建基于云计算的新型安全技术

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。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，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。

4. 卫士通有望在军工业务中获得未来新一轮增长极

4.1 与国内云计算龙头阿里云合作，打造“网安飞天”安全云切入军工领域

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。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，未来军队自主可控云计算平台中获取新一轮增长极。

4.2 公司是 5G 军用标准制定者，未来有望成为独家军用 5G 通信服务商

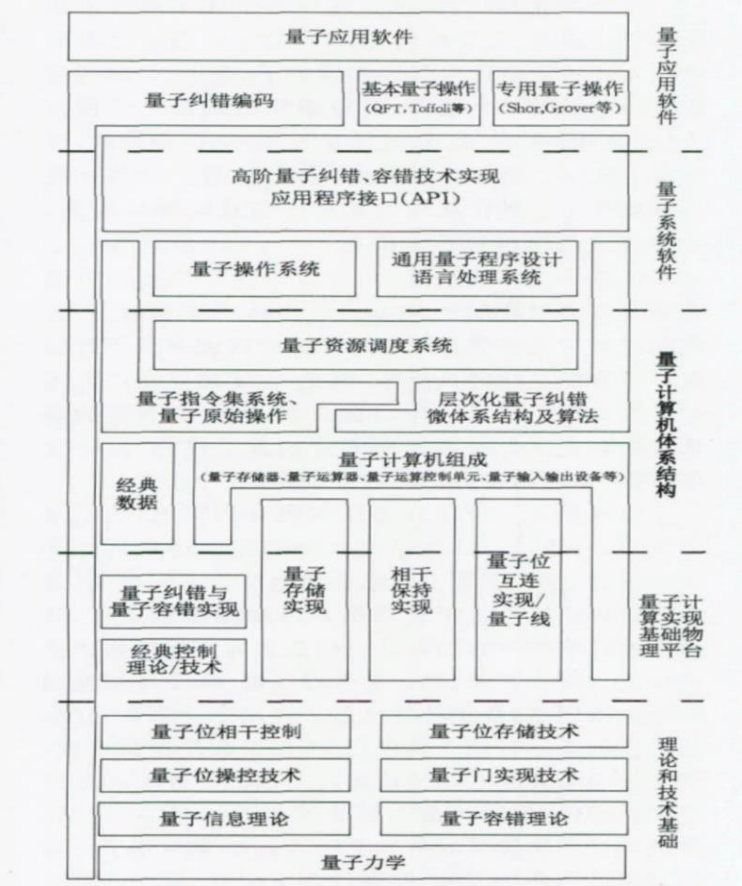
卫士通作为一家以密码技术为基点的公司，在加密领域领域默默耕耘二十余年，奠定了国内安全加密行业绝对龙头地位。卫士通提前进行技术战略卡位，成立 5G 安全专项推进组，重点开展 5G 密码应用等研发，依托于密码技术这一核心优势，确立以密码为基础的统一信任体系，构建多元分立的数据防护模型,建立整体性的安全服务基础设施,形成面向垂直行业的 5G 安全解决方案，为未来军队 5G 专网通信提供服务。

4.3 量子层级研究推动未来网络安全发展

4.3.1 量子计算机与量子加密概念的引入

量子计算机可理解为一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。也就是说某个可以处理和计算量子信息，并且运用的是量子算法的装置就可以被称为量子计算机。目前量子计算机分为两类，一是通用量子计算机，二是专用量子计算机。第一类通用量子计算机的进展比较缓慢，对于当前的使用密码尚不能构成威胁；而专用量子计算机的商业化发展迅猛，已有多家公司推出相关产品，目前谷歌和 IBM 都在加紧研发中。

图 17：量子计算机体系结构与量子计算中其他部分的关系



资料来源：公开网络，东兴证券研究所

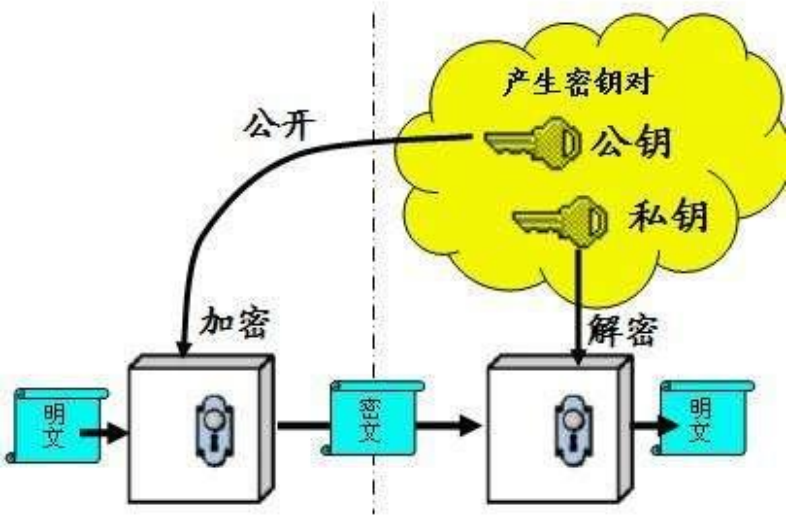
量子加密技术是利用量子的物理特性,基于光的偏振现象,海森堡测不准原理和量子不可克隆定理的基础上发展起来的新型加密技术。它的理论体系包括量子秘钥分发、量子加密算法、量子秘密共享和量子认证等。

同使用数学算法的当代加密技术相比,基于量子力学原理的量子加密技术是更加严密和安全的保密手段。量子加密技术是信息安全的前沿领域,因为具有广泛的应用领域和良好的应用价值,近年来吸引各国政府和科研部门的高度重视，目前为止,它仅在短距离内可以通过验证,随着技术的进步,未来将有可能实施长距离的量子加密。量子加密技术的成果虽然不少,但是离广泛的实用推广还有很长的距离,与经典加密技术相比还很不健全,许多方面有待于深入研究。

4.3.2 量子计算机的发展现状

通用量子计算机器件进展缓慢。对于通用量子计算机，人们最期待的就是其运行 Shor 算法破译 RSA 等公钥密码的能力。但就目前来看，通用量子计算机还没有破译实际运行的 RSA 等公钥密码的能力。公钥密码体制就是使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。

图 18：RSA 算法



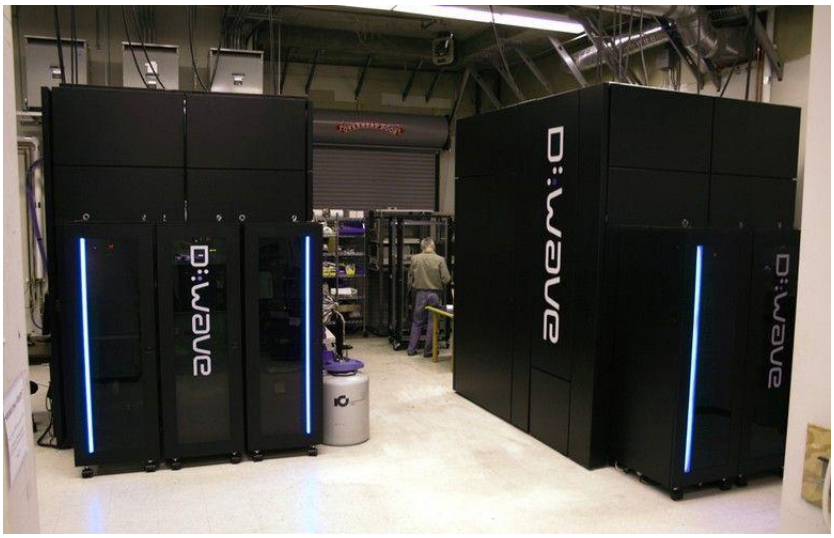
资料来源：公开网络，东兴证券研究所

目前对于量子效应的操控仍是难题。一旦受到例如来自外界的杂散光子或振动造成的干扰，量子计算将崩溃。这是因为人们在物理实现中破坏了量子系统的封闭性，使量子计算系统与环境产生了耦合从而引起量子信息向环境泄漏。在如何消除这方面的影响上，目前理论与实际仍有较大的差距。

专用量子计算机商业化进展迅速。其原理是基于量子人工智能独特的量子隧穿效应(quantum tunneling effect)，完全不同于通用量子计算机，也不能运行破译RSA密码的Shor算法，对Shor算法破译RSA密码没有任何直接帮助。专用量子计算机的发展迅猛主要由于其在商业化中的市场需求。

根据《Nature》2011年5月的报道，Lockheed Martin率先以1 000万美元（液氦冷却装置价格另计）购置了第一台128 Qubit的商业化加拿大专用量子计算机D-Wave One，用于先进武器设计、F35战机缺陷分析、开发和测试雷达、航天和航空器系统等。2013年5月，Google正式宣布以1 500万美元购买了年初推出的第二代512 Qubit商业化专用量子计算机D-Wav Two，专用量子计算机正式进入商用阶段。

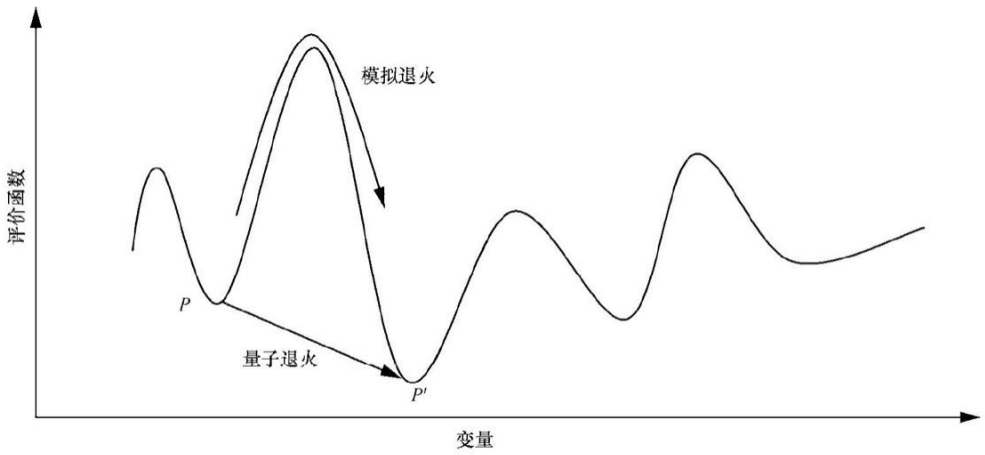
图19：专用量子计算机D-Wave One



资料来源：公开网络，东兴证券研究所

D-Wave One 可以实现量子退火算法。洛马购买的第一代商业化加拿大量子计算机已经成功实现了具有量子隧穿效应的量子退火算法。量子波动使量子具有穿透比它自身能量更高的势垒能力，即量子隧穿效应。量子退火算法利用量子波动产生的量子隧穿效应可以使算法跳出局部亚优解、有望以较大概率逼近全局最优。这是与模拟退火及其他众多计算搜索算法相比的一个独特优势。但从量子器件角度看，完成量子退火的难度较大。

图 20：量子退火与模拟退火示意图



资料来源：公开网络，东兴证券研究所

D-Wave 公司的设计构思非常巧妙，利用量子隧穿效应实现了量子退火，可以将一些组合优化问题求解的 NP 难题在多项式时间解决，《Nature》认为可广泛用于密码学、人工智能、图像搜索、图像识别和模式分类、金融风险分析、生物信息学、情感分析等众多领域。**正是由于专用量子计算机有望解决许多实际问题，其近些年的发展才会如此迅猛，并将持续高速的发展下去。**

IBM 宣布三年后上市第一台量子计算机。其实 IBM 已经研究量子计算机数十年，但目前这个三年时限仅仅是预测，不过量子计算机到来的日子确实越来越近了。有一个例子可以解释量子计算机的能力，要破解现在常用的一个 RSA 密码系统，用当前最大、最好超级计算机需要花 60 万年，但用一个有相当储存功能的量子计算机，则只需花上不到 3 个小时。不论真正意义上的第一台量子计算机何时到来，量子技术的发展方向是肯定的，一旦成功研发意味着旷阔的市场空间。

4.3.3 卫士通在量子加密领域的进展

公司已布局后量子密码技术研发。公司 2017 年年报指出，公司通过商用密码实验室增强了密码基础理论研究和前沿技术研究的能力，并且开展了后量子密码的研究。根据是否基于量子物理原理，量子安全选项可划分为两种基本类型，即后量子密码与量子加密技术。后量子密码，又被称为抗量子密码，是被认为能够抵抗量子计算机攻击的密码体制。此类加密技术的开发采取传统方式，即基于特定数学领域的困难问题，通过研究开发算法使其在网络通信中得到应用，从而实现保护数据安全的目的。后量子密码的应用不依赖于任何量子理论现象，但其计算安全性据信可以抵御当前已知任何形式的量子攻击。

公司大股东中国网安已布局、开展“量子密码”的相关研究。中国网安依托中国电科 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。

4.3.4 新局势下卫士通密码业务未来市场空间巨大

目前量子加密技术发展缓慢，主流 RSA 算法仍将控制市场。虽然从理论上量子计算机会对 RSA 算法进行破译，但目前的技术水平还不足以实现。因此，继续发展 RSA 等公钥密码仍是密码安全领域的核心，公司将在国产化密码算法方面迎来机遇。目前公司已将国产通用算法运用到部分领域，并将继续推动公司主营业绩提升。

表 3: 公司密码产品

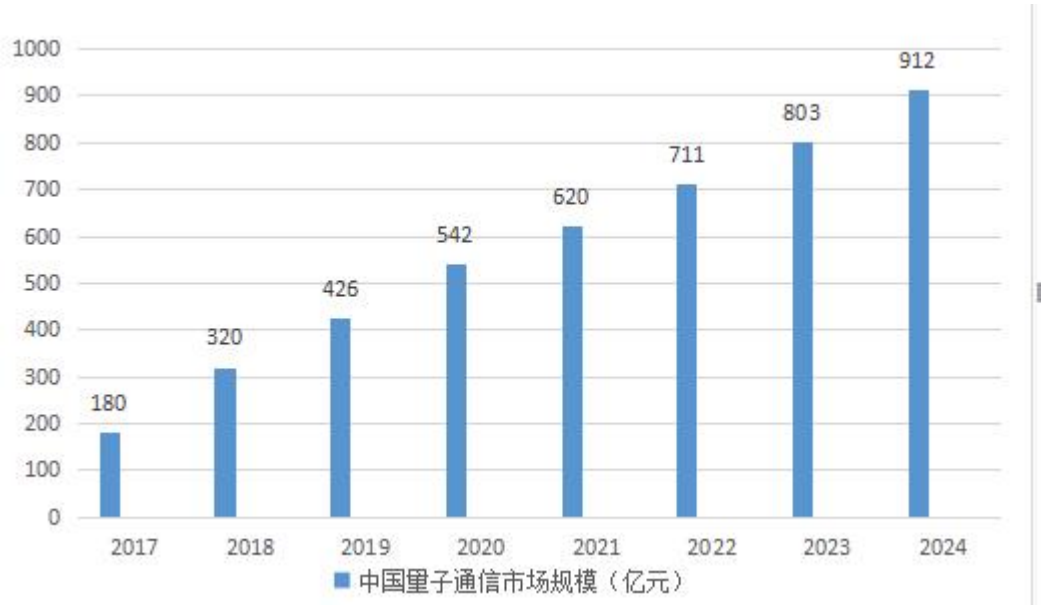
领域	产品	领域	产品
芯片	商用 PCI-E 密码卡	模块	智能密码钥匙
系统	密钥管理系统	设备	云服务器密码机
	金融 IC 卡数据准备系统		签名验证服务器
	金融 IC 卡密钥管理系统		金融数据密码机
	统一密码服务系统		服务器密码机

资料来源：公司官网，东兴证券研究所

公司有望竞争量子通信未来长期千亿市场空间。量子加密技术可以有效的运用到量子通信领域，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 21：我国量子通信市场规模预测



资料来源：公开网络，东兴证券研究所

5. 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，维持公司“强烈推荐”评级。

6. 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。