东兴证券 DONGXING SECURITIES

新领导新气象，紧抓网络攻防不放松

——卫士通（002268）深度报告系列之三

2019 年 01 月 24 日

强烈推荐/维持

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

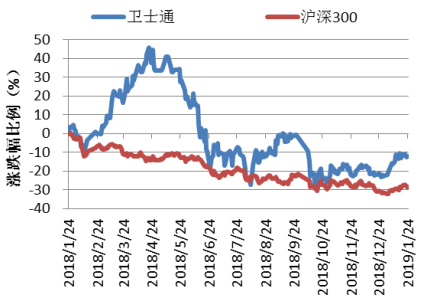
010-66554018 Zhangzq_yjs@dxzq.net.cn

执业证书编号: S1480117080010

交易数据

52 周股价区间（元）	16.30-34.72
总市值（亿元）	170.52
流通市值（亿元）	165
总股本/流通股（非限售）（百万股）	838/810
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、《卫士通深度报告：安全可控助力安全运维增长，密码优势有望引领自主可控弯道超车》2018-11-11

2、《卫士通深度报告：布局军用云计算，打造业务新成长极》2018-09-17

3、《卫士通深度报告：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》2018-08-21

报告摘要：

1、新董事长到位，业绩拐点来临。新任中国网安和卫士通董事长卿昱同时兼任中国电科 30 所所长，未来将有力推动卫士通与 30 所之间的业务协同和利益分配。她在网络安全领域建树颇多，曾任中央网信办安全协调局副局长和三零盛安副董事长，将有力推动中国网安的央企安全运维业务和军用云计算安全业务。

2、加密业务即将爆发。预计老一代密码机在 2022 年全部更换完毕，市场规模约 500 亿元。考虑初期换装速度慢，2019 年保守估计带来 20 亿元的增量。央企安全运维方面，招商局项目落地后，公司目前与 20 余家央企洽谈，如果 2019 年新签 10 家央企，按每家央企 1-2 亿的运维费用测算，新增约 15 亿收入。

3、网安飞天云和 5G 安全业务新增利润点。中国网安“飞天云”在 2018 年获得试点订单，目前已调试完毕，2019 年预计新增 5 处试点，利润率较高。5G 专网网络铺设方面，公司有望成为 5G 通信安全的总包方，初期毛利率较高。公检法信息化方面，卫士通有望在民事取证业务上发力。该业务规模远高于刑事取证，其核心数据存储有望使用中国网安的密码技术防止泄密。

4、网战先锋，代表了新军事变革方向。当前，中国网安在加密，央企安全运维，网安飞天云，5G 专网通信，IPV6，身份认证，电磁干扰等多条网络攻防业务链上形成了网络攻防闭环，战略位置至关重要，并且做到了真正自主可控。公司初具美国 Fire Eye（火眼公司）雏形，在网络攻防、网络监测预警方面已成为“网络最强蓝军”，将是未来我国网络对抗、网络武器和网络战的主力先锋。

5、根据上述几大领域业务拓展情况，我们预计卫士通在 2019 年迎来业绩拐点。我们预测公司 2018 年、2019 年和 2020 年收入分别为 27.15 亿元、52.27 亿元和 76.92 亿元，归母净利润分别为 1.60 亿元、5.47 亿元和 8.08 亿元，EPS 分别为 0.19 元、0.65 元和 0.96 元，维持公司“强烈推荐”评级。建议重点关注。

风险提示：安全运维推广不达预期，政务云竞争激烈，5G 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	2,715.10	5,226.90	7,691.92
增长率（%）	12.21%	18.80%	27.05%	92.51%	47.16%
净利润（百万元）	155.75	169.05	160.30	547.30	807.85

增长率（%）	4.69%	8.54%	-5.18%	241.42%	47.61%
净资产收益率（%）	10.46%	3.94%	3.64%	11.44%	15.12%
每股收益(元)	0.36	0.21	0.19	0.65	0.96
PE	53.99	92.18	101.66	29.78	20.17
PB	5.65	3.79	3.70	3.41	3.05

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. 新董事长出身三十所业务骨干，技术背景在全国网安领域名列前茅

新任中国网安董事长卿昱第一份工作即在三十所，学者出身多年从事网络安全工作，未来将有效推进传统加密领域业务，理清业务链实现卫士通与三十所业务之间的业务协同和分配问题；在网络安全领域建树颇多，着眼于云计算安全等全新安全领域，有望在推动网安云计算业务的顺利推广特别是军工领域；曾任三零盛安副董事长，熟悉网络安全服务业务，且曾担任网信办安全协调局副局长，在央企安全运维领域将加速业务推进。

1.1 长期从事网络安全研究，根植三十所党政领域贡献巨大

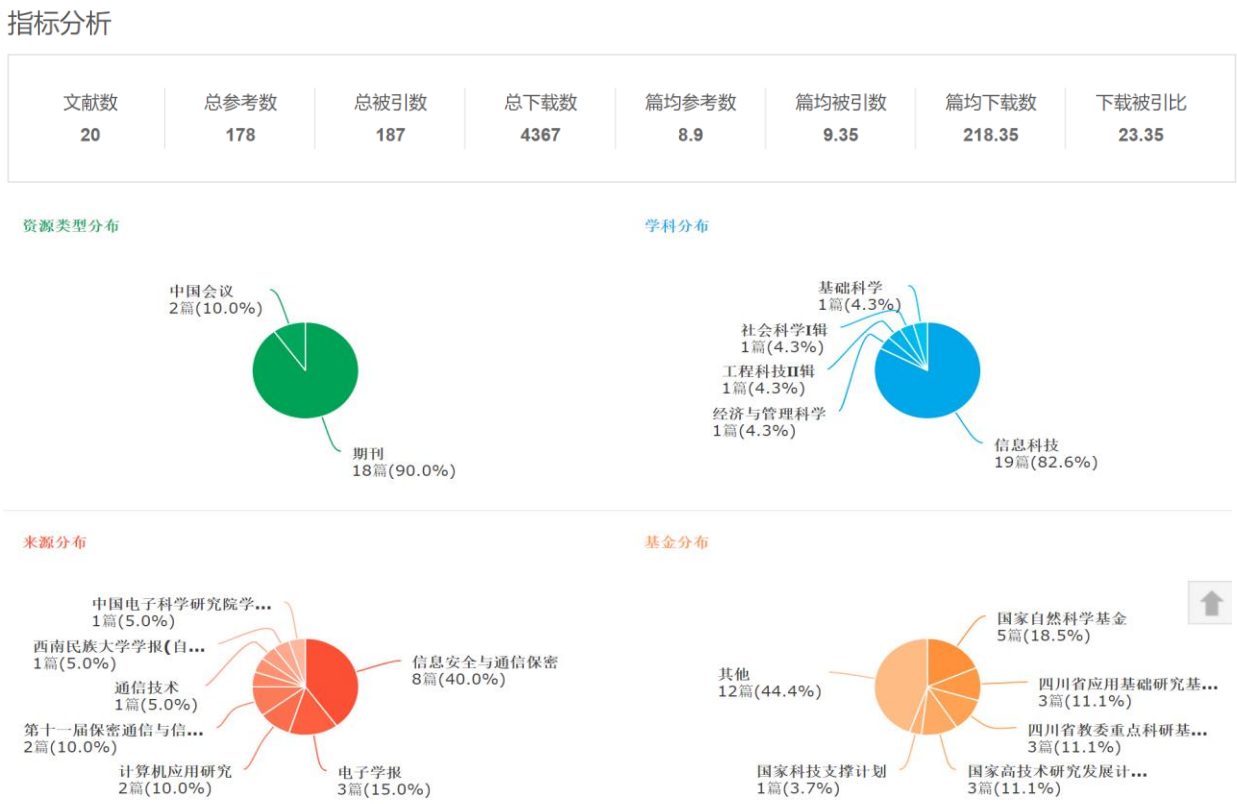
卿昱出生于 70 年代，1995 年毕业于上海交通大学获得信息与控制工程系硕士学位。大学毕业后,分配到中电科第三十研究所(原电子部三十所)工作,历任所一室副主任、主任。2000 年出任三零卫士安全软件公司副总经理，从一个纯技术研究的高级工程师转换为公司高层管理者。后该公司与三零信息工程公司整合为三零盛安，于是 2002 年后担任三零盛安副总经理。工作期间，她主持的某个管理系统项目，获部级科技进步三等奖；担任“九五”国防某个重点科研项目开发总体负责人；主持过数据网某个项目的设计、实施和开发，该项目获部级二等奖。

曾调任中央网信办网络安全协调局任副局长，后回中电科集团任中国电子科技网络信息安全公司副总经理，中国电子科技集团公司第三十研究所所长，国家电子政务专家委员会委员。主持和参与了多项国家和军队重大项目，共获军队科技进步一等奖二次，部级科技进步二等奖一次，著有《云计算安全技术》，公开刊物上发表多篇论文。

1.2 多篇核心论文涵盖多个安全领域，尤以云计算安全为核心

知网上对新任董事长的论文进行总结，可以看出学者型领导确实在多个领域都有建树，如云计算安全、信息安全系统评估、安全通信、身份认证、P2P 网络蠕虫、P2P 网络架构分析、可信计算等。

图 1：卫士通董事长论文指标分析

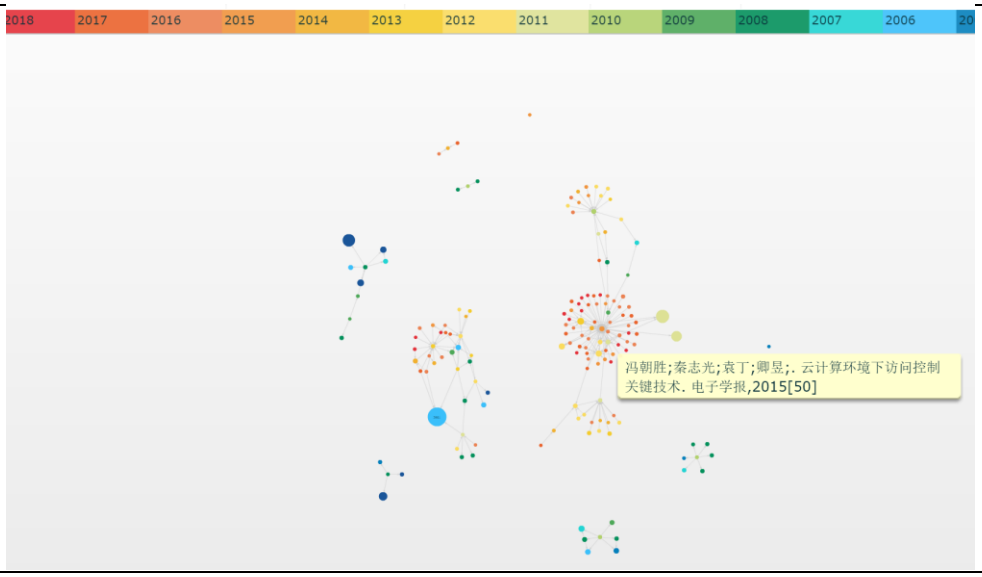


资料来源：中国知网，东兴证券研究所

文章以期刊为主，主要发表在信息安全与通信保密上，基本全部分布在信息科技领域。其中参与众多国家级自然科学基金研究项目。

其中尤以云计算安全为近期研究重点，被广泛引用。2017 年在第五届指挥控制大会上，在进行题为“外军云计算安全保密体系研究及启示”的主题演讲时，卿昱详细介绍了美军的云计算发展概况，重点剖析了美军在建设模式及演进、管理模式及在云安全技术体系方面的特点。同时还分享了五点启示和思考：多安全级别、多建设管理模式并存的费效比最高；标准先行，推进军用云计算安全基线的制定；打造开放式的云计算安全服务体系，推进军民融合；高度重视监管能力的打造，确保多云并存体系的安全可靠；应对即将到来的大数据挑战，先行启动大数据安全体系和标准的研究。

图 2：卫士通董事长论文相关数据



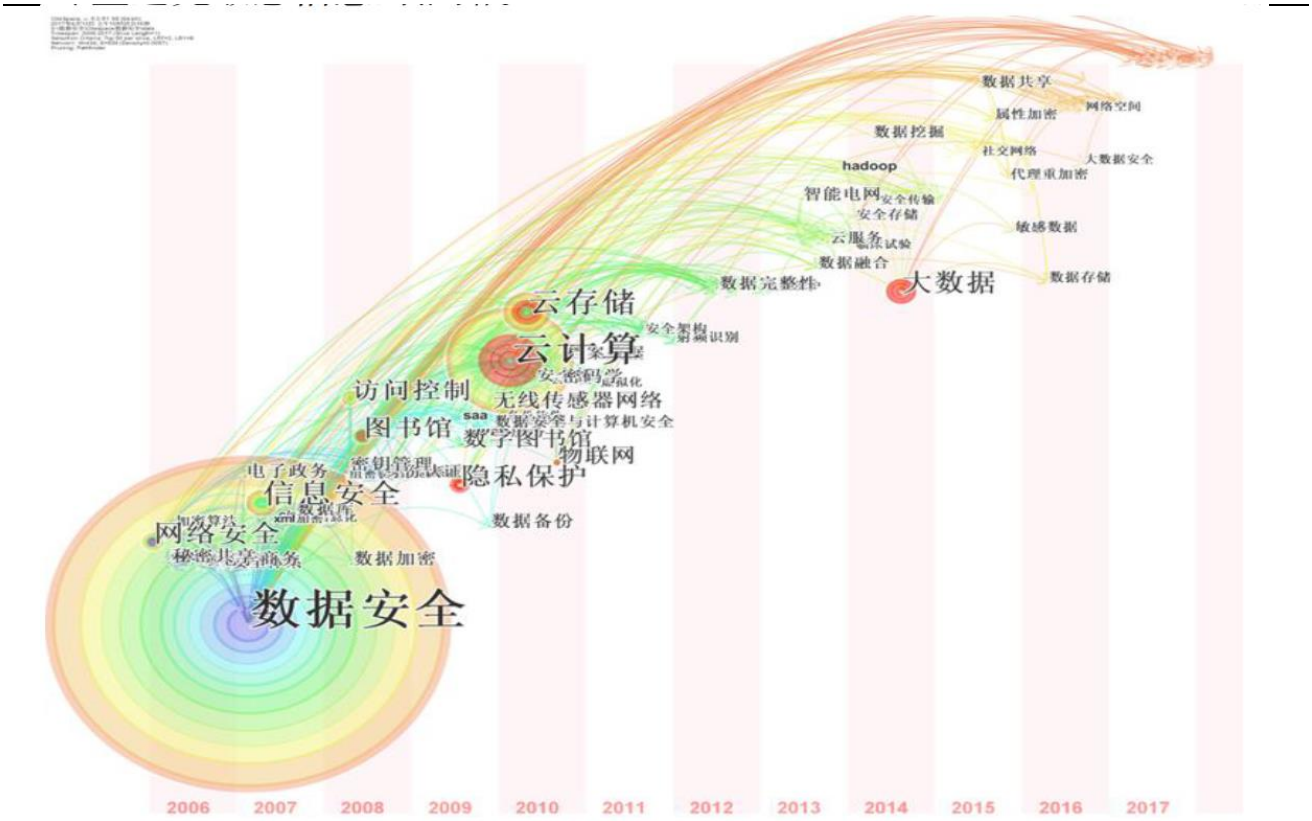
资料来源：中国知网，东兴证券研究所

2. 传统安全业务领域受益自主可控，加密新技术引领行业前进

“中兴事件给我们敲响了警钟，让我们科技公司意识到，我们在这方面和国外还是有很大的差距。我们的信息技术有一些‘命门’，并不完全掌握在自己的手上。”在 2018 年网络安全技术高峰论坛上卿昱表示，在网络安全技术上，我们的信息基础还是不够强健的，比如说操作系统、CPU 等还有很大一部分依赖于国外的产品，“目前，国家也在积极发展‘自主可控’的软件产品，我们希望通过‘自主可控’的技术研发，使得自身信息技术的基础更加坚实，为网络新技术的发展创造更安全、更可靠的环境。

2006 年出现的“数据安全”、“网络安全”和“信息安全”字体较大，且与后续出现的关键词联系紧密，说明数据安全研究是以“网络安全”和“信息安全”为主要研究对象。随着时间推移，该领域的研究对象正在发生变化，依次出现了以“隐私保护”、“云计算”、“云存储”、“物联网”和“大数据”为主的研究对象。

图 3：数据安全主题时区分布图



资料来源：网络资料，东兴证券研究所

可以看出，随着技术的发展，新一代数据安全与云计算、大数据等新技术联系紧密，作为数据安全研究核心的密码领域，也要与时代发展契合，发展新一代密码技术。

2.1 密码领域卫士通具备顶级资质

我们国家将信息安全划分为三个等级：核密、普密和商密。其中核密最高，普密次之，商密最低。核密指国家党政领导人及绝密单位的安全级别，此领域不存在任何商务行为。普密是指国家党政军机关的信息安全级别，此领域安全设备由国家指定的五家研究机构负责研制工作，具有市场实力的只有三家：中电科 30 研究所、数据所、总参 56 所。另外两家是空三所，中船 722 所。

普密和商密这两种信息的保护要求不一样，普密可以用于保护一定范围的国家安全信息，对国家秘密保护的强度包括它的手段和技术。从密码角度来说保护国家秘密信息的时候所采用的密码必须是普密级以上的，普密设备从管理上要求对普密产品、设备（包括研制、生产、销售普密产品的企业）的管理非常严格，应用圈子相对较小。

商密用于保护企业级的商业秘密，技术上不一定比普密低，但商密产品的管理程度不如普密，应用产品多，应用面广（如 VPN）。国家规定商密禁止操作任何国家秘密以上的安全信息。

2.2 商密领域多点开花

卫士通公司以“密码国内第一、安全国内一流”为产品体系创新的目标，以商用密码产品为代表，研发和推出了一批在业界具有竞争力的拳头产品，其中多款产品处于国内首创、国际先进水平。

2.2.1 金融领域

金融领域，商用密码已大规模应用于金融 IC 卡、网上银行、跨行交易等主流银行业务。智能终端在高安全、大额度的交易应用需求中，必须采用数字签名、加密等措施，保护交易的安全性。云计算安全直接关系到我国关键信息基础设施的安全，因此，必须充分发挥密码在云计算安全中的核心支撑作用。

金融领域，在金融行业，以国密算法改造为切入点，积极开发满足用户需求的密码设备，在为用户提供密码产品的同时，为银行国密算法升级改造提供整体安全解决方案。

2.2.2 移动互联网领域

终端加密领域，卫士通的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。除党政军客户外，卫士通积极布局安全支付手机这一市场，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 Mate8VoLTE 安全手机。次年中国移动卫士通 4GVoLTE 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 Mate9 在内的 3 款安全手机已正式发布。

2.2.3 云计算领域

在云计算领域，与阿里云合作的网安飞天安全云平台，强强联合，利用阿里云的底层技术和卫士通本身的密码优势，采用密码设备虚拟化技术，研发应用于云计算环境，能实现密码计算资源的集约利用、动态伸缩、迁移，并满足政府、企业、金融行业、云服务提供商等对于云数据加密保护、云内部安全管理、密钥管理及身份认证安全需求的云密码卡、云密码机和云密钥管理。

卫士云是公司子公司卫士通信息产业股份有限公司提供的云计算产品。

图 4：卫士云

资料来源：网络资料，东兴证券研究所

知名 IT 市场研究机构 IDC 对 2019 年安全产品和服务趋势进行预测，以密码技术为中心的主动防御、身份安全及数据安全将成为网络安全产业发展的新风向。

图 5：IDC2019 年网络安全市场预测

资料来源：网络资料，东兴证券研究所

针对未来网络安全威胁，面向市场和用户关切，卫士通加速向网络安全服务商转型，打造了国内首个基于国产密码的一体化高安全云平台—卫士云，为党政、中央企业、军队等高安全需求用户提供包括高安全 IaaS、体系化安全服务、安全 SaaS 服务在内的一系列专业的安全云服务。

1）主动防御——卫士云为用户提供基于态势感知的网站防护服务

卫士云遵循“防监固评” 四位一体安全理念，采用业界领先的云防御、防篡改、主机加固等技术，从网络层、主机层、管理层的安全需求出发，为用户提供可弹性扩展的安全服务、精细控制的主机安全和应用安全，以及智能化自动化的安全运营服务，多维度构建基于态势感知的主动防御体系。针对客户的不同需求，目前主要为客户提供“卫士·云御”（云防御平台、在线监测、应急响应等）、“卫士·磐石”（主机安全系统、网页防篡改系统、网络安全态势感知、Web 应用防护系统等）两大系列的产品服务。卫士云网站防护解决方案荣获 2018 中央企业网络安全与工业互联网十佳解决方案。

2）身份安全——卫士云提供专业的统一身份认证服务

卫士云统一身份认证服务基于多账户统一、多证书统一和多终端统一的“三统一”理念，提供覆盖用户管理、身份认证、授权管理、应用管理和日志审计的“5A"级身份

服务功能，结合便捷的接入流程和统一的管理服务入口为政企用户提供安全便捷的服务体验，并以此为根基构建可信的身份生态，筑牢信息化及数字转型的身份新边界。

3）安全移动办公——卫士云提供企业微信加密、橙讯、橙讯安全邮等安全应用

企业微信加密服务是卫士通着力打造的企业云安全可信加密解决方案，主要解决企业微信中潜在的安全风险，服务采用国密算法对企业核心业务数据进行端对端的二次加密，实现从终端、通信链路到云服务平台三位一体的安全防护，保证企业核心业务数据在云端传输以及存储的安全。

橙讯作为基于商用密码的安全即时通信软件，通过安全的加密通话、即时通信、企业通讯录为用户提供商密级的端到端即时加密通信和基于终端的个人信息保护等安全服务，打造安全、快捷、高效的协同办公体验。

橙讯安全邮支持国际通用算法、自主知识产权的商用密码算法，采用端到端安全邮件技术，邮件发出到接收全程内容加密，为用户提供公众级、商密级等多层次安全邮件服务。

2.3 为信息产业自主可控提供安全基础

习近平总书记高度重视国家信息技术发展，围绕“突破互联网核心技术、实现信息技术产品安全可控”多次作出重要部署。在 2018 年 4 月召开的全国网络安全和信息化工作会议上，总书记提出，“核心技术是国之重器。要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。要抓产业体系建设，在技术、产业、政策上共同发力。要遵循技术发展规律，做好体系化技术布局，优中选优、重点突破”。

卫士通作为安全可靠技术和产业联盟中六家安全厂商之一，为适应国家战略、技术趋势和产业形势，通过整合优势资源，重点打造了网络安全管控与态势感知、信任服务、网络安全、安全云运营平台、安全移动办公、安全终端、安全芯片、密码模块和自主可控系列产品。

公司 5 月份研制的中华卫士自主可控万兆交换产品，核心部件全部国产自主化，包括龙芯 2H 芯片、盛科交换芯片、CPLD 等自主可控核心部件。

2.4 后量子密码研制迫在眉睫

事实上，具有强大密码破解能力的量子计算机近年来已经不断取得实质性进展，研究者们普遍认为应该尽早部署能够抵御这种威胁的后量子密码技术，从而将全球信息网络系统面临的总体风险降至最低。所幸中国网安集团作为全国加密技术领头羊，早早就布局量子密码技术，使得我国的信息系统不至于在量子计算机出现后出现无法加密的局面。

2.4.1 量子计算能力对于现行密码系统的潜在冲击

在当前的网络通信协议中，使用范围最广的密码技术是 RSA 密码系统、诸如 ECDSA/ECDH 等 ECC 密码系统以及 DH 密钥交换技术，这些通用密码系统共同构成了确保网络信息安全的底层机制。但这些对于经典计算机来说足够“困难”的问题必将在可预期的将来被实用型量子计算机轻易破解。

图 6：量子计算机对当前加密算法的威胁

加密算法	类型	作用	潜在量子计算能力威胁造成的冲击
AES	对称密钥	加密	增大密钥长度
SHA-2, SHA-3		哈希功能	需要更大输出量
RSA	公钥加密	数字签名 密钥生成	丧失安全性
ECDSA, ECDH（椭圆曲线密码）	公钥加密	数字签名 密钥交换	丧失安全性
DSA（有限域加密）	公钥加密	数字签名 密钥交换	丧失安全性

资料来源：网络资料，东兴证券研究所

2.4.2 量子计算的前溯性威胁使部署后量子密码技术需求更加紧迫

如果现在的通信网络流量遭到窃听并被存储下来，未来潜在的对手利用量子计算能力，就能对这些通常处于加密状态的信息进行破解，从而在多年以后将威胁范围追溯到当前。

在 2015 年的报道中，《自然》杂志引用荷兰情报与安全总局（DutchGeneral Intelligence and Security Service）负责人的观点认为，不法攻击者现在开始拦截和存储金融交易数据、个人电子邮件及其他互联网加密流量行为，“并不会让人感到意外”。除此之外，大规模数据收集毫无疑问已经成为某些国家政府组织的例行性工作。根据斯诺登揭露的资料，美国和英国情报机构正在通过“上游”计划，利用海底光缆登陆站毫无遗漏地收集约占全球联网流量 99%的光缆通信信息。《连线》杂志早在 2012 年就披露美国国家安全局已经开始在犹他州新建一座数据中心，其有能力将互联网自诞生以来产生的所有流量全部保存下来，从而使其成为一种战略资源，供美情报机构在掌握量子计算能力后进行开发。因此，虽然量子计算机的出现可能还需要数十年，但这种能力本身已经具有了现实性威胁。

3. 安全运维受益等保 2.0，核心资质助力央企业务爆发

3.1 等保 2.0 利好整体信息安全行业，特别是安全运维领域

图 7：公安部关于《网络安全等级保护条例》公开征求意见


中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China

返回首页 | 信息公开 | 办事服务 | 警民互动

公安部关于《网络安全等级保护条例（征求意见稿）》公开征求意见的公告

时间：2018年06月27日 字体：【大】【中】【小】

公安部关于《网络安全等级保护条例（征求意见稿）》
公开征求意见的公告

为贯彻落实《中华人民共和国网络安全法》，深入推进实施国家网络安全等级保护制度，经广泛征求意见，反复研究修改，公安部会同有关部门起草了《网络安全等级保护条例（征求意见稿）》。为保障公众知情权和参与权，凝聚各界共识和智慧，提高立法质量，现向社会公开征求意见。

公众可登陆公安部网站（网址：http://www.mps.gov.cn）查阅征求意见稿，有关建议可在2018年7月27日前通过电子邮件方式发送至djbht1@163.com，或传真至010-66262319。

公安部

2018年6月27日

资料来源：中华人民共和国公安部，东兴证券研究所

3.1.1 等保 2.0 与网络安全法

网络安全等级保护已经进入 2.0 时代，等级保护制度已被打造成新时期国家网络安全的基本国策和基本制度。应急处置、灾难恢复、通报预警、安全监测、综合考核等重点措施全部纳入等保制度并实施，对重要基础设施重要系统以及“云、物、移、大、工”纳入等保监管，将互联网企业纳入等级保护管理。

等保 2.0 的标准是国内非涉密信息系统的安全集成标准，网络安全法是作为法律、中国信息安全的基本法。网络安全法中明确的提到信息安全的建设要遵照等级保护标准来做建设。

3.1.2 等保 2.0 的不同及要求

从名称上来看，原信息安全等保标准叫做信息安全等级保护制度，现在 2.0 叫做网络安全等级保护制度。这意味着，等级保护上升到了网络空间安全的层面。这个名称的改变意味着等级保护的对象全面升级：之前保护的对象是计算机信息系统，而现在上升到网络空间安全了，除了包含之前的计算机信息系统，还包含网络安全基础设施、云、移动互联网、物联网、工业控制系统、大数据安全等对象。

另外一个重点是等保定级方式的改变，就是等级保护 2.0 的定级并不是用户自主定级，而是要参照定级指南进行定级，这是需要特别注意的一点。

等保 2.0 将等保工作的技术要求和管理要求细分为了更加具体的八大类：物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全;全策略和管理制度、全管理机构和人、安全建设管理、安全运维管理。而等保 2.0 在以上基本要求之外，提出了云安全、移动互联网安全、物联网安全、工业控制系统安全、大数据安全等网络

空间扩展要求，且每个部分都有详细的安全标准。这些都是等保工作需要做的重点工作。

图 8：公安部关于《网络安全等级保护条例》公开征求意见

资料来源：中华人民共和国公安部，东兴证券研究所

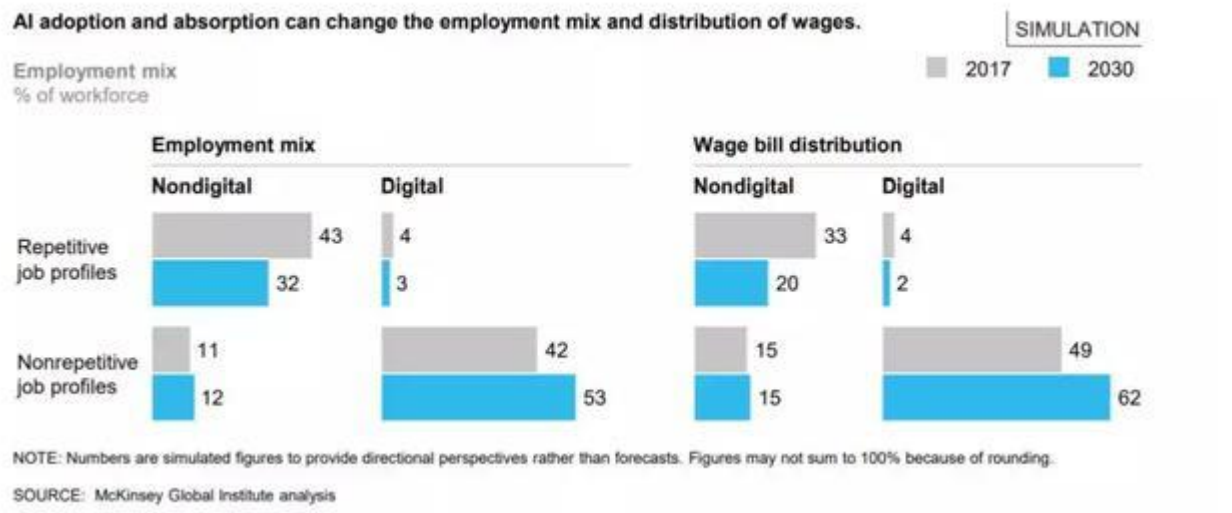
等保 2.0 也特别新增了外包运维管理的管理要求，选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，应在与外包运维服务商签订的协议中明确所有相关的安全要求。如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。对公司内部安全运维的要求降低和对外包运维的要求增多，这也从侧面体现了等保 2.0 对安全服务的认可，体现了安全服务正越来越成为一种趋势。

3.2 AI 技术的发展带来外包趋势

AI 技术和大数据等新技术投入实用，实现了从学术研究到产业落地的飞跃，工作自动化程度明显提升，技术支持型平台企业有望承担更多的劳务外包型业务。在网络安全领域，表现为可针对网络威胁实现全面威胁监测、实时安全防护、及时风险预警和自动化应急处置，减少相关人员工作量，提升自动化水平，降低运维成本。

AI 技术的普及使得自动化或劳务外包更加普遍，特别是脑力或者体力上的重复性劳动。麦肯锡全球研究院的最新研究表明，重复性任务和少量数字技术为特征的岗位需求，可能会从总就业占比的 40%下降到 2030 年不到 30%；而对非重复性活动或高水平数字技能的工作岗位需求，从大约 40%上升到超过 50%。

图 9：麦肯锡全球研究院最新研究结果



资料来源：网络资料，东兴证券研究所

3.3 以招商局安全运维项目为起点，19 年力争央企安全运维市场

国内网络安全产业传统上以满足党政军需求为主，不同厂商之间缺少协同联动，这种碎片化的发展方式一方面适应了前期体量不大的网络安全产业发展需要，另一方面也给国内网络安全产业发展带来了负面影响——目前尚不能为大型或超大型组织机构提供“一体化”的网络安全整体解决方案；另一方面，新兴的互联网巨头对于网络安全的认知和努力，又主要集中于保障庞大基数用户的隐私数据和自身业务的连续性；如何解决中央企业这一类大型或超大型组织的网络安全整体保障难题，是中国网安卫士通作为网络安全“国家队”必须面对的挑战。

央企承担着金融、电力、运输、核工业等国家经济命脉，在各基础设施领域推动产业互联网发展、实现信息化的过程中，卫士通背靠中国网安集团肩负信息安全国家队职责，为央企提供 7*24 小时的线上线下运维服务和实时、动态的主动防御服务。在九月份完成招商局集团网络信息安全整体保障服务项目建设后，10 月 10 日以卫士通人员为行政总师，中国网安网络监测预警事业部、卫士通公司、三零卫士公司选派 38 人组成精英团队，最终实现了“分钟级发现、分钟级预警、分钟级处置”的安全服务。其中表现优异的是网监部的金牌蓝军网络攻防团队 MS509，通过对系统实施黑白盒测试来查找漏洞；从事主动防御的基于人工智能的态势感知系统；基于多层语义网络的关联分析引擎；自主可控的从芯片到系统的网络防火墙、密码管理机等信息安全产品线。招商局整体安全运维保障项目的圆满成功，预示着卫士通有望在 200 亿市场空间的央企安全运维市场取得领先的市场份额。

3.3.1 卫士通负责央企安全运维总包，背靠中国网安集团资源肩负信息安全国家队职责

网络安全整体保障模式的及时出现，正是为解决中央企业关键信息基础设施的整体保障问题。整体保障服务的愿景是为大型企业和超大型企业提供一体化的网络安全整体保障解决方案，以专业化的服务、低密度的投入、透明化的弹性接入为中央企业在新一轮数字浪潮中的转型升级保驾护航。作为中国网安五大战略业务之一，网络安全整体保障服务也是卫士通由安全产品提供商向综合安全服务运营商转型的重要战略支

点。作为唯一专业从事网络信息安全国有上市企业，卫士通在整个国家网络安全发展的阶段中，面临着“三重使命”：

第一重使命是作为网络空间安全捍卫者，支撑国家攻防力量对比的专业组织；

第二重使命是作为中央企业网络信息安全产业的代表，通过创新的模式和过硬的能力，做大做强网络信息安全国有资本；

第三重使命是作为中央企业关键信息基础设施保障的亲历者，必须着力解决市场现有网络安全供应商不能满足大型和超大型组织整体保障需求的问题，推动网络安全市场供给侧结构性改革，带动网络安全产业的高质量发展。

2018 年卫士通与招商局集团签订业内首个网络安全整体保障服务合同，开启了以网络安全服务取代安全设备为交付物的服务新模式。服务内容既包括传统的安全设备运维、安全防护系统建设、安全信息系统集成，还包括业界还处于探索阶段的攻防实战对抗、威胁情报聚合、事件实时分析、攻击事件复盘、业务影响沙盘推演等，人才队伍奇缺，技术标准、工作机制无一现成经验可借鉴，作为中央企业总资产第一的招商局集团，对集团网络信息安全的要求高、标准严，整体保障服务的质量时刻面临着“严苛”的审核与挑战。

在招商局项目中，卫士通人员作为行政总师，携手中国网安集团各公司精兵强将，圆满完成了任务。2018 年 9 月 27 日，《招商局集团网络信息安全整体保障服务项目》评审会在北京顺利召开，专家组一致同意该项目通过建设实施阶段性验收评审；后续服务不断改进，实现了“分钟级发现、分钟级预警、分钟级处置”的服务目标要求，得到用户的肯定和赞扬；2018 年 12 月 14 日上午，招商局集团信息中心组织召开了《招商局集团网络信息安全整体保障服务项目》半年服务（3 月 13 日至 9 月 13 日）评审会。招商局集团高层领导在听取服务年度汇报会议后，对服务理念、服务方式十分认同。

在招商局工作经验的基础上，与军工、能源、电信、交通等重点领域的 20 余家中央企业和地方重要国有企业开展整体保障业务合作，开展“数字电科”网络安全整体保障建设，与中国远洋海运、中广核集团、上海诺基亚贝尔等签订整体保障战略合作协议，与南方电网、中国电建、北汽集团等开展整体保障相关项目合作。

图 10：卫士通负责招商局安全运维总包

资料来源：网络资料，东兴证券研究所

3.3.2 中国网安集团网络监测预警事业部是集团五大新动能之一，MS509 网络攻防团队曾获央企网安大赛最强蓝军称号

中国网安的网络监测预警事业部诞生背景是，2013 年，美国“棱镜”计划被曝光，看似遥不可及的美国情报机构竟然与全世界每个人的隐私都发生了关系，而斯诺登关于“美国一直从事针对中国个人和机构的网络攻击”的言论也促使国家层面开始思考与探索应对网络空间发展不平衡局面的措施举动。自中国网安成立伊始，公司高层就积极思考、筹划和开展前沿布局，依靠自身掌握的核心能力，将网络监测预警作为公司发展的五大新动能之一，同时，抽调专业和骨干力量，正式组建网监事业部，着力开展网络监测、态势感知、安全情报、综合运维管理、应急响应等领域的技术研究、产品孵化以及行业解决方案打造，以支撑国家在关键信息基础设施领域的网络安全发展战略需要。

图 11：中国网安集团网监事业部职能

资料来源：网络资料，东兴证券研究所

网监事业部以支撑国家重大项目、产业类项目试点示范、渠道推广等为契机，深度参与国防、政府、行业、中央企业等重点安全项目的调研、设计和建设，进一步巩固了专业的安全运维管理和网络运维管理的总体地位，实现了不少安全保障领域从无到有的突破，打造了中央企业网络安全整体保障服务体系建设的样板案例，为今后在网信、公安、工信等领域开展应用推广打下坚实的基础。

事业部在做集成业务时，在军方通过统一接口标准，让各厂商安全设备各司其责，形成体系化的协同能力；在民口的中央企业网络安全整体保障服务项目中，也是吸纳众多网络安全厂商的优秀产品，通过统一的大数据底座及统一的威胁研判和态势呈现平台，形成体系化的整体交付能力，满足用户“分钟级发现、分钟级处置”的安全防护目标。

图 12：中国网监事业部

资料来源：网络资料，东兴证券研究所

整合网监事业部核心产品所形成的“中央企业网络安全态势感知与监测预警平台”，入选 2018 年工信部大数据产业发展试点示范项目；针对中国电科下属单位网站进行整体安全保障，全力打造的网站云防御平台，形成的“基于态势感知的网站安全解决方案”被评为公安部十佳方案；在第一届全国网络舆情（音视频）分析技术邀请赛上，代表中国网安获得视频关键词检索第一名；协助四川省经侦总队在 2018 年公安部全国经侦大比武中，取得第 2 名的优秀成绩。

特别是事业部的 MS509 团队，从 2015 年起就支撑中国网安成为中央网信办网络安全检查支撑单位之一，活跃于业界的网络攻防舞台，先后获得 2018 年中国电科集团第一届攻防大赛团体一等奖和最强红军称号，中央企业网络安全技术大赛最强蓝军称号等。

3.3.3 三零卫士为央企提供互联网舆情和威胁情报数据服务

上海三零卫士信息安全有限公司（简称三零卫士）成立于 2001 年 7 月，是中国电科网络信息安全有限公司（简称中国网安）旗下专业的综合性网络安全服务提供商。

作为国内最早从事网络安全行业的前瞻者和领军者，为我国党政军、医疗卫生、教育、石化、金融、交通、电力等行业客户提供全面、系统、安全特色显著的综合性信息化及网络安全服务。三零卫士现有员工 700 余人，全国累积客户约 1500 家。总部设在上海，在杭州、广州、北京、成都、武汉、南京等地设有分支机构。

三零卫士目前形成了“网络安全服务”、“工控系统网络安全服务”、“社会信用平台建设和大数据服务”及“互联网舆情和威胁情报数据服务”等四大核心业务板块。

图 13：三零卫士

资料来源：网络资料，东兴证券研究所

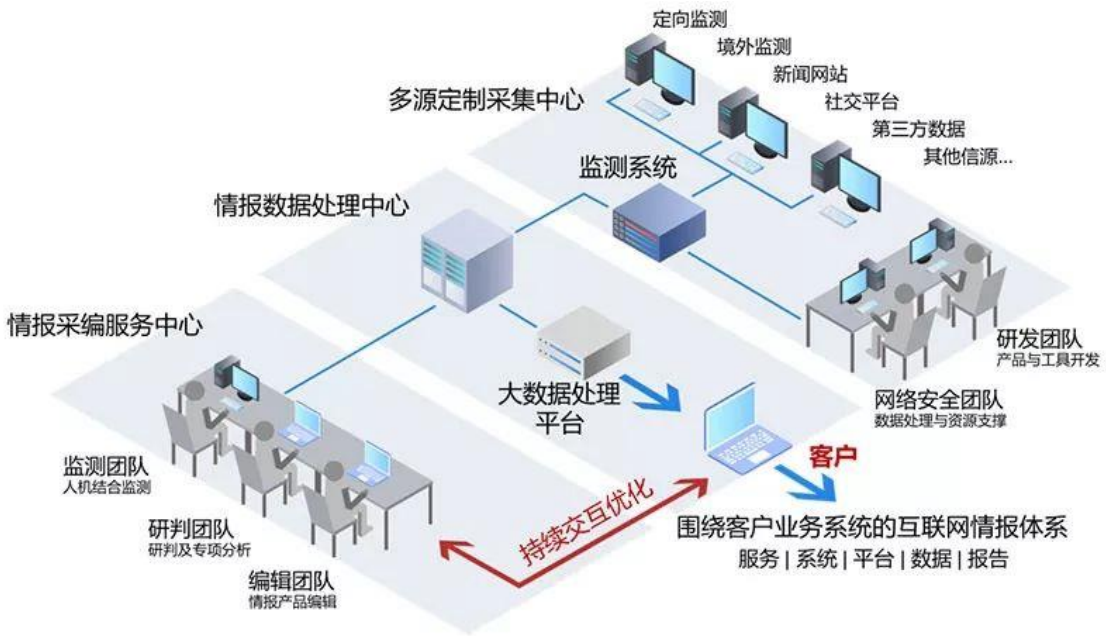
三零卫士以网络信息安全服务作为业务形态，为不同行业客户的核心业务应用信息系统提供全生命周期的整体安全保障。三零卫士通过 S-Team 安全研究团队、互联网网络安全预警与应急中心、自主知识产权的云服务产品，构筑"0"时畅享服务体系，在网络安全服务中为用户实现“0”延时、“0”操心、“0”距离的，三“0”目标。

图 14：三“0”目标

资料来源：网络资料，东兴证券研究所

互联网、大数据、云计算相继揭开了智能时代的序幕，新时代新常态中，网络安全已经不仅仅是网络本身的安全，更是国家安全、社会安全、基础设施安全、城市安全、人身安全等更广泛意义上的安全。国家、社会各行各业的网络安全问题一定存在并将持续存在，在保护与威胁的博弈中主导先机，才是智能时代的安全之道。三零卫士互联网情报业务以“情报助力安全博弈”为使命，“大数据融合创新”为技术导向，提出了“安全应对，情报先行”的网络空间安全理念，形成了以成都为中心辐射全国的互联网情报服务网。

图 15：互联网情报体系



资料来源：公开网络，东兴证券研究所

三零卫士建立的中国网安互联网情报服务中心，提供四类情报。

图 16：中国网安互联网情报服务中心提供四类情报

资料来源：公开网络，东兴证券研究所

三零卫士顺利完成北京奥运、上海世博、广州亚运、G20 峰会、南京青奥、世界互联网大会乌镇峰会等国家级重大活动信息安全保障任务。

3.3.4 安全运维三亮点

1）防护功能是它的雷达，能通过网络设备、安全设备、服务器日志全采集，实现日志威胁全监测与网络流量全解析，达到监测无盲区；

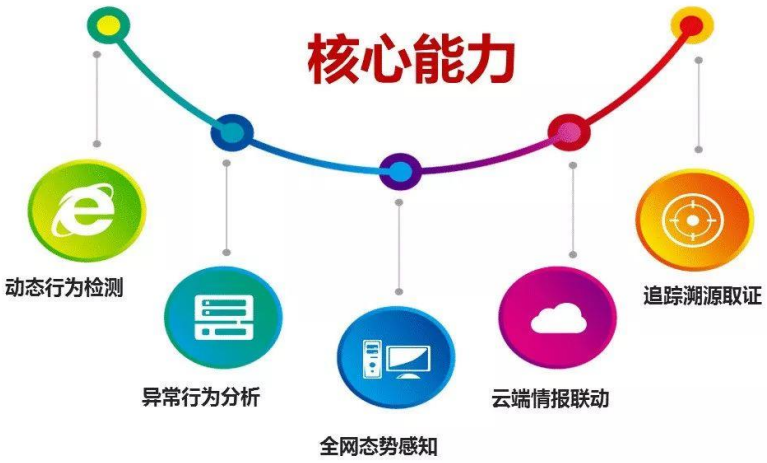
中国网安高级威胁监测防御体系：APT 攻击为是当今网络的主要威胁，他可通过精准的社工情报、定向的攻击手段和高级的渗透技巧，实现对目标的长期性、持续性的控守，或获取数据资产，或执行破坏任务。通常选择有价值的“猎物”：如党政、军队、金融、能源、交通、大型企业等国家关键信息基础设施。其中，由网络监测预警事业部打造的中国网安高级威胁监测防御体系，可通过涵盖网络侧、服务侧、终端侧等多类系统的监测、分析一体化解决方案，全力防御 APT 攻击。

图 17：高级威胁检测防御体系

资料来源：公开网络，东兴证券研究所

高级威胁监测防御体系拥有行为仿真、机器学习、态势感知、情报联动和追踪溯源等核心能力，建立了覆盖事前预警、事中监测和事后追溯的监测预警体系。

图 18：高级威胁检测防御体系核心能力



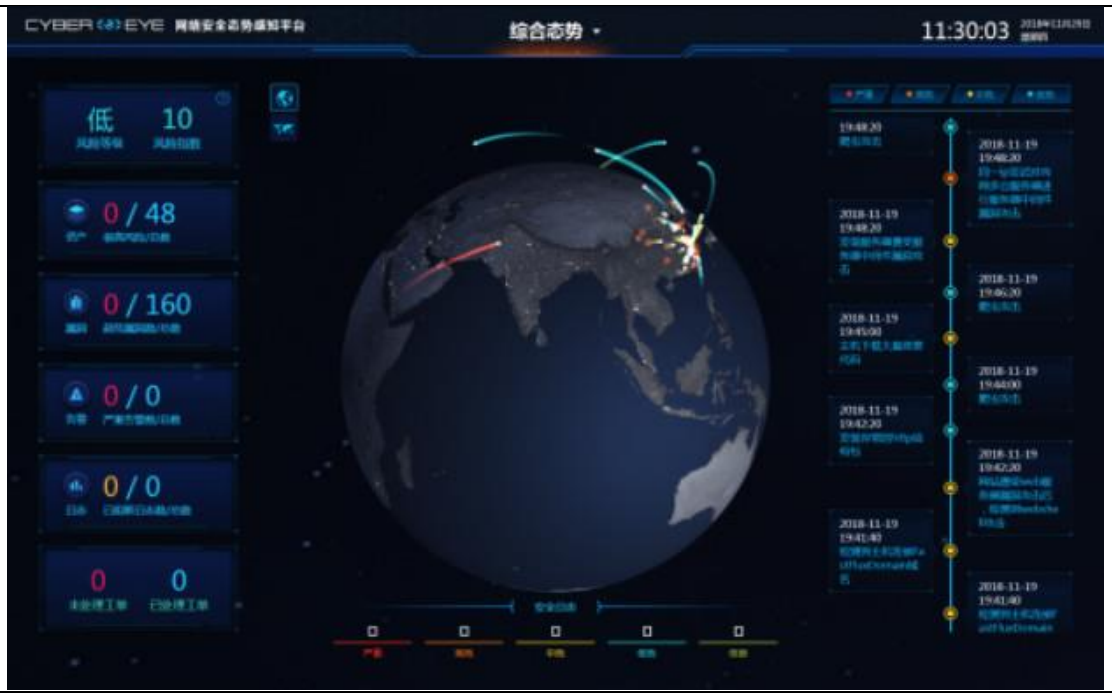
资料来源：公开网络，东兴证券研究所

高级威胁监测防御体系能基于 40Gbps 的海量数据收集能力，通过多级分布式的部署，以 DNS 异常解析模型、DGA 检测模型、HTTP 隐蔽流量模型等机器学习手段，开展对全网已知威胁和异常行为的全面检测，还原攻击过程，感知全网威胁态势。高级威胁监测防御体系还能开展行为仿真分析，对捕捉的文件样本进行网络行为、文件行为等的动态检测，以指令级的分析粒度，强化在本地对未知威胁的快速识别能力。另外，高级威胁监测防御体系还能以“找线索，循过程，查证据，追源头”为使命，通过态势感知、行为分析、威胁情报和追踪溯源等体系化对抗手段，持续增强关键信息基础设施遭受 APT 攻击时的应对能力。

2）网络防火墙、Web 防火墙、安全接入 VPN、终端安全管控、运维堡垒机、服务器安全加固等自主可控产品；

3）基于态势感知的全局协同，利用大数据安全分析、关联分析、机器学习、情报分析等方法是它的云端协同，能对网络威胁进行监测、分析和预警响应，并与防护型网关进行协同联动处置。

图 19：中国网安网络安全态势感知平台



资料来源：公开网络，东兴证券研究所

随着信息技术的高速发展，网络安全事件频发，网络攻击已经从黑客个人行为升级为有组织的、国家与国家之间的网络信息化能力的较量。对于日益严峻复杂的网络安全威胁，广大政府机关、企事业单位迫切需要一个忠实的守护神帮忙捍卫。中国网安网监事业部针对广大政府机关、企事业单位的网络安全建设需求，结合普遍的网络安全现状，打造了“监测防御处置”一体化、“多引擎”智能化的全天候全方位态势感知平台。

图 20：全天候全方位态势感知平台

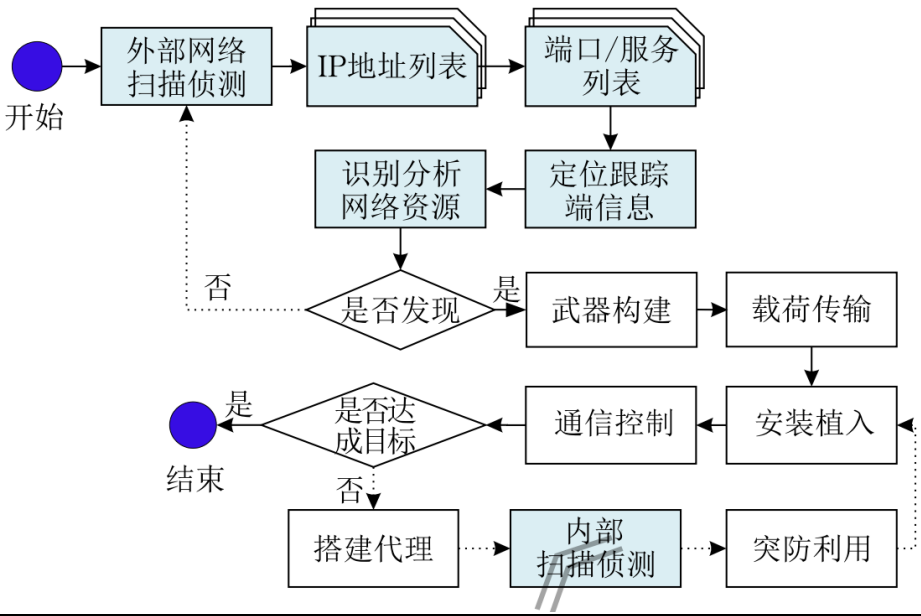
资料来源：公开网络，东兴证券研究所

网络安全态势感知平台以多元异构大数据采集、智能关联分析、机器学习等技术为核心，形成了统一的大数据安全底座，集成了检测防护引擎，融合了态势感知厂商能力，可实现全面威胁监测、实时安全防护、及时风险预警和自动化应急处置，为广大政府机关、事业单位提供态势感知“预警机”。与其他态势感知厂商的能力融合，集多家感知引擎之所长，做到威胁监测的全面覆盖。整合引入国内外顶尖的威胁情报厂商，为广大政府机关、企事业单位提供私有化、定制化的情报数据。充分结合用户实际的安全运维处置工作流程，实现自动化威胁处置的工作流程。

4. 网络攻防技术是我国提升网络安全的重中之重

习近平总书记指出，网络安全的本质在对抗，对抗的本质在攻防两端能力较量。从实际情况来看，对抗的“主战场”则集中于关键信息基础设施。目前国内关键信息基础设施运营单位主要分为三类：第一类是由党政军各部门负责运营的网络信息系统，主要运行与国家管理职能相关的业务系统；第二类是以中央企业和地方重要国有企业运行的网络信息系统，主要运行公共服务和企业重要资产的业务系统；第三类是以“BAT”为代表的大型互联网厂商，主要运行与个人有关的隐私数据和业务信息。

图 21：网络攻击流程图



资料来源：公开网络，东兴证券研究所

4.1 国际网络安全产品市场发展现状与趋势

伴随着计算机和信息技术的发展，网络空间作为实体空间的拓展，日益成为各国竞相争夺的“第五空间”。各国纷纷建立专门的网络部队，发展网络武器，网络战趋势明显。网络空间的虚拟性、无疆性造就了网络空间安全威胁来源的多重性、复杂性。伴随着不断提高的网络安全重要性和快速多样化的网络空间攻击能力，网络安全产品市场正在火热兴起，无论是军用还是民用，网络安全产品都在快速更迭。

4.1.1 网络战争投入日渐增多

2007 年，爱沙尼亚政府及其机构遭受大规模网络攻击，被认为是“网络空间的第一次战争”；2012 年火焰(Flames)和蠕虫(Stuxnet)的出现标志着更多的国家开始使用网络武器；2013 年，美国官员表示，网络攻击已经取代恐怖袭击成为美国国家安全的最大威胁。网络安全正在成为各国国家安全的重点，各国网络安全的维护也正面临着巨大威胁，网络安全问题在政治、军事等议程上的日渐突出，也给全球带来了巨大的经济市场。2011 年，全球范围内的公共和私营网络安全支出大约 600 亿美元。也就是说，全球网络安全支出相当于全球军费开支的 3.5%，2015 年全球网络安全市场的价值已突破 1100 亿美元，预计在接下来的 3 到 5 年内还会以每年 10%的速度增长。全球行业分析师公司（Global Industry Analysts Inc）认为，全球网络安全市场的价值到 2018 年会达到 1500 亿美元。汇信公司（Vision gain）估计全球网络安全市场的价值在 2016 年约为 1200 亿美元，并估计规模更为有限的全球网络战市场的价值为 400 亿美元，且有继续增多的趋势。

4.1.2 传统军火商进入网络安全领域

国际网络安全产品市场的发展与主权国家和非国家行为体网络安全需求的发展相一致，也与其网络安全攻防能力的发展相适应，在此背景下，许多传统的军火公司和新兴信息技术公司纷纷进军网络安全产品市场。

一方面，网络攻击具有低成本、高回报的特点，不同于常规武器和核攻击，网络攻击能力的获取门槛低，国家总体实力的强弱并不必然决定网络空间攻击能力的强弱。网络空间的虚拟性与无限广阔性决定了任何国家、地区、公司甚至是个人都有可能在某一方面获得网络攻击能力，

另一方面，一些常规武器市场面临的实际困难，越来越多的国家和军火生产商、军事服务公司投身于网络攻击武器和网络防护能力的研究中。网络安全市场的兴起促进了网络空间斗争的日趋激烈，主要的军火生产公司不断收购网络安全供应商，从事网络武器研究。

这些公司一进入市场就体现出各自的技术区别，分别在不同的方面提供服务，一方面与公司的自身基础密切相关，另一方面，网络空间的多层次造成不同公司的不同优势。

表 1：电子政务移动办公系统面临的主要安全风险

网络安全业务类型	子类别	公司

网络和数据保护软件及业务	加密方案 管理识别鉴定方案 系统配置 数据丢失防护 恶意软件检测及清除	BAE 系统公司 CACI 国际公司 计算机科学公司 欧洲宇航防务集团 ManTech 国际公司 雷神公司 科技应用国际公司
测试与模拟业务	渗透测试及脆弱性评估 商业/经济影响分析 认证/技术符合性评估	BAE 系统公司 计算机科学公司 欧洲宇航防务集团 洛克希勒马丁公司 ManTech 国际公司 科学应用国际公司
培训与咨询服务	个人培训咨询服务：基础设施设计、计划与实施方案、网络安全政策定义等	BAE 系统公司 CACI 国际公司 计算机科学公司 欧洲宇航防务集团 洛克希勒马丁公司 ManTech 国际公司 科学应用国际公司
	网络监视软件和服务 事故管理、数字取证和数据恢复方案	BAE 系统公司 计算机科学公司 欧洲宇航防务集团 L-3 通信公司 诺斯罗普格鲁曼公司

资料来源：公开网络，东兴证券研究所

根据斯德哥尔摩国际和平研究所的统计，“SIPRI100 强”中许多关键武器项目的主要承包商都进入了网络安全市场，例如 BAE 系统公司、欧洲宇航防务集团、洛克希德．马丁公司等，通过不同的网络安全业务战略，逐步在网络安全市场占据重要的一席之地。比如洛克希德．马丁公司与主要的信息技术和网络安全公司(迈克菲、微软、惠普等)结成了战略联盟。这些网络军事服务公司在网络安全市场获得巨大的收入，尽管相对常规武器的收入来说小得多，但是考虑成本与收益的角度，网络安全市场的高收益率吸引了更多的公司或军火供应商进入网络安全市场。

4.2 美国借助人工智能等新一代技术，网络攻防领域继续维持优势

2017 年 5 月 12 日，勒索病毒 Wanna Cry 在世界范围内爆发，短短 4 天之内，就有包括中、美、英、葡、俄、意等 150 余个国家遭受大规模攻击，超过 10 万家组织和机构被攻陷。中国有近 3 万家机构受到影响，涉及高校、加油站、火车站、自助终端、邮政、医院，甚至政府企事业办事终端等领域，损失之严重为近年来所罕见。Wanna Cry 是借助了“永恒之蓝”的力量实现大规模传播。据悉，“永恒之蓝”属于美国国家安全局（NSA）旗下的黑客组织——“方程式组织”（Equation Group），且仅仅是该组织“永恒王者”、“永恒浪漫”、“永恒协作”等系列针对个人终端的黑客工具之一，它们可以远程攻破全球约 70%的 Windows 机器。

4.2.1 特朗普政府的网络安全政策

朗普政府上台后，重新评估美国网络安全状况，检讨奥巴马政府网络安全政策，逐步进行网络安全政策调整。特朗普政府通过加强网络攻防能力建设，减少多边投入，并对中国单边施压来迎合国内政治需要，维持美国在网络空间主导地位。总体上，特朗普的网络安全政策调整符合其“美国优先”的执政理念。

特朗普政府上台后，提出“以实力谋和平”(Peace through Strength)原则，旨在通过加强军事能力建设强化对潜在敌手的威慑，维持美国的全球领导地位。网络安全领域同样如此。特朗普政府认为，美国必须确保在网络安全领域的主导地位不受挑战。

为加强网络安全能力建设，特朗普政府提出三项优先行动计划：一是提高网络溯源、追责和快速反应的能力；二是强化网络工具，招募、培训和维持能胜任各类工作的专业队伍；三是加强政府相应职权与工作程序的整合，提高报复性反击能力，与国会就情报和信息共享、规划与运营以及网络工具发展等问题进行合作。

2017 年 12 月 18 日，特朗普政府出台任内首份《国家安全战略报告》。在这份报告中，网络安全的地位得到明显提升，被视为“关系美国未来繁荣与安全”的重要议题。

2018 年 2 月 12 日，特朗普政府公布《2019 财年预算草案》，计划未来向信息技术和网络安全领域投入 800 亿美元，包括网络信息系统建设、网络人才培养以及为网络任务部队提供必要资源等。

2018 年 5 月，美军网络司令部完成升级，日裔陆军上将保罗·中曾根(Paul Nal(asone)为新任司令。该司令部拥有 133 支网络任务部队(Cyber Mission Force，简称 CMF)，所有网络任务部队有望在 2018 年底全面投入运转。2018 年 8 月 18 日，特朗普宣布将美军网络司令部升格为第十个联合作战司令部，地位与战略司令部、太平洋司令部等持平。

4.2.2 美国积极利用人工智能打造网络攻防能力

美国充分认识到人工智能已经逐步进入到商业化阶段，已经将人工智能置于维护其全球主导军事大国地位的核心。美国各相关部门已经开始研发智能化网络攻防武器，白宫甚至还推出了人工智能国家战略，将智能化网络攻防武器纳入国家战略之中。

美国现任总统特朗普在 2016 年 4 月的一次竞选演说中提到，美国需要将 3D 打印技术、人工智能和网络战一体化用于军事，以便让美军在 21 世纪无以匹敌。

表 2：电子政务移动办公系统面临的主要安全风险

时间	事件
2015.9	美国国防高级研究计划局（Defense Advanced Research Projects Agency，DARPA）在 2015 年 9 月举行的未来技术论坛中，将自主人 工智能列为四大议题之一加以讨论。
2016.1	美国战略与国际问题研究中心在其《国防 2045：为国防政策制定者评估未来的安全环境及影响》中，也将“先进计算/人工智能”列为五大新兴与颠覆性技术之首。
2016.4	美国现任总统特朗普在 2016 年 4 月的一次竞选演说中提到，美国需要将 3D 打印技术、人工智能和网络战一体化用于军事，以便让美军在 21 世纪无以匹敌。
2016.5- 2016.7	美国白宫更是在 2016 年 5-7 月内召开 4 次公开研讨会，并于 9-12 月陆续发布了包括《为人工智能的未来做准备》、《人工智能研究开发战略规划》、《人工智能、自动化与经济》等在内的 6 份文件，将其提升为国家级战略，提出政府要监控其他国家人工智能发展情况，政府和私营部门、安全部门应确保生态系统在应对智能对手时能够保证安全性和恢复能力，实现有效、高效的网络安全，把自主和半自主武器系统纳入了美国国防计划。
2016.8	1 支名为 Mayhem 的机器网络攻防战队与另外 14 支人类顶尖战队上演了首次人机黑客对战，并一度超过 2 支人类战队，成为网络安全领域的 AlphaGo 事件。

资料来源：公开网络，东兴证券研究所

4.2.3 网络攻击链

杀伤链最初由美国空军参谋长 Ronald Fogleman 将军于 1996 年空军协会研讨会上提出的。通常而言，杀伤链主要分为 6 个阶段：

发现（Find）锁定（Fix）跟踪（Track）定位（Target）交战（Engage）评估（Assess）

距离杀伤链开始越近，阻断攻击的效果便越好。例如，攻击者获得的信息越少，其他人就越不可能使用这些信息来完成接下来的攻击过程。

1） 而网络杀伤链该理念最初是由 Lockheed Martin（洛克希德·马丁）公司提出的，描述了有针对性的攻击阶段，同样防御者也可以利用它们来保护组织的网络。

图 22：洛克希德马丁定义网络杀伤链

资料来源：公开网络，东兴证券研究所

小偷需要先去目标地进行侦察，然后试图渗透其中，最终获取实际战利品之前需要经过的几个步骤。想要使用网络杀伤链来防止攻击者潜入你的网络中，你需要对网络中发生的事情具有一定程度的了解和可见性。你需要知道什么时候不应该发生什么事情，如此你才可以设置警报来阻止攻击行为。

洛克希德·马丁公司参考美国防部信息作战（IO：Information Operation）小组的应对方案，将网络防御类型分为探测、拒止、干扰、弱化、欺瞒、破坏六种。应对网络攻击的类型中，探测是指发现、识别入侵者的行为，拒止是指阻止攻击者的接入，干扰是指阻挠破坏攻击者的入侵信息流，弱化是指降低攻击效率及攻击效果，欺瞒是指通过捏造虚假信息，使攻击者做出错误的判断，破坏是指使攻击者或攻击工具受到损伤，丧失应用功能，无法恢复原状。

图 23：针对杀伤链的应对方式

应对类型 攻击流程	探测 (Detect)	拒止 (Deny)	干扰 (Disrupt)	弱化 (Degrade)	欺瞒 (Deceive)	破坏 (Destroy)
侦察 (Reconnaissance)	网络分析（Web Analytics）	防火墙访问控制表(Firewall ACL)				
武器化 (Weaponization)	网络入侵检测系统(NIDS)	网络入侵防护系统(NIPS)				
散布 (Delivery)	警惕用户(Vigilant user)	代理过滤片(Proxy filter Patch)	在线视频（In-line AV）	队列（Queuing）		
恶用 (Exploitation)	基于主机入侵检测系统（HIDS）	补丁（Patch）	数据执行保护(DEP)			
设置 (Installation)	基于主机入侵检测系统（HIDS）	根目录监禁（"chroot" jail）	视频（AV）			
命令与控制 (C2)	基于主机入侵检测系统（HIDS）	防火墙访问控制表（Firewal l ACL）	网络入侵防护系统(NIPS)	限定蠕虫（Tarpit）	DNS 重定向（DNS redirect）	
目标达成 (Actions on Objectives)	日志审计（Audit log）			服务质量（Quality of Service）	蜜罐（Honeypot）	

资料来源：公开网络，东兴证券研究所

2）美国防部的“网络安全杀伤链”

美国防部在 2015 年发行的《网络安全测试与评估指南》6 中援引美国防部防御分析研究所(Institute for Defense Analysis)的资料，提出了包括网络攻击与防御主要活动、目的等内容的“网络安全杀伤链(CSKC: Cyber security Kill Chain)”。在 CSKC 的攻击流程中，没有网络杀伤链中的设置阶段，且在目标达成阶段之后，追加了维持阶段。CSKC 的防御者应对类型与网络杀伤链的应对类型相同。

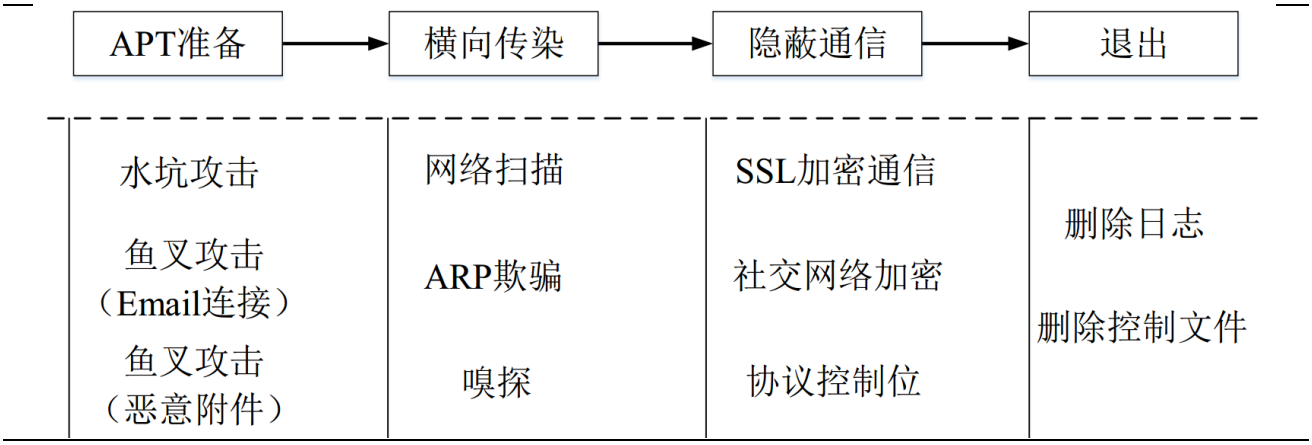
图 24：美国国防部定义的网络安全杀伤链

资料来源：公开网络，东兴证券研究所

4.3 APT 及主动防御将改变原有网络安全市场结构

传统的网络防御技术是一种静态的、被动的防御技术，它面临着如下问题：静态的网络安全防御技术只能抵御已知攻击，无法抵御未知攻击，如 0day 漏洞等；静态的网络安全防御技术的防御能力是静态的，不能随着环境的变化而不断变化，而攻击者的攻击能力是不断提升的，这就造成了防御方的被动局面；静态的网络安全防御技术很难阻挡攻击者的扫描行为，而这往往是攻击的第一步，从而让攻击者获得了目标网络或系统的足够信息；面临攻击方日益复杂的攻击，如 APT 攻击，即使传统安全技术的有效组合也很难抵御；静态的网络安全防御技术通常是用来进行边界防护并抵御外部攻击，却无法有效抵御内部攻击。

图 25：APT 流程及主要攻击手段



资料来源：公开网络，东兴证券研究所

APT 攻击，即高级持续性威胁(Advanced Persistent Threat)是利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。APT 攻击的原理相对于其他攻击形式更为高级和先进，其主要体现在精确的信息收集、高度的隐蔽性以及使用各种复杂的目标系统或应用程序漏洞等方面。

APT 攻击的主要特点可以概括为以下三个：1．攻击时间长，而且对一个攻击目标实施重复攻击。2．传统所使用的安全防护措施难以应对 APT 的攻击。3．APT 攻击能够识别出攻击目标的防护措施，并且找出防护措施的漏洞，从而使自身的攻击能力得到进一步强化。

洛克希德-马丁的网络杀伤链（Cyber-Kill-Chain，网络攻击生命周期），可以被用来识别和防止 APT 入侵。网络杀伤链模型用于拆分攻击者的每个攻击阶段，在每个阶段都采用对应的特征用于识别。在越早的杀伤链环节阻止攻击，防护效果就越好，修复的成本和时间损耗就越低。例如，攻击者取得的信息越少，这些信息被第三人利用来发起进攻的可能性也会越低。因此，可以根据网络杀伤链模型制定分层分级的安全防护网络体系。

我国网络安全方面的技术发展越来越接近国际水平，但是整个产业的发展仍然落后于主流国家。由于市场、社会认知以及产品特殊性等原因，需求端的企业，总是更倾向于购买传统安全产品，如防火墙、防病毒软件等，市场对服务类的网络安全服务类产品的需求不强烈。基于流量审计的下一代网络安全产品在国内目前仍处于起步阶段。然而，基础安全类产品只能进行被动防御，信息技术未来发展趋势是大数据、物联网、移动互联网等，这需要网络安全以平台化为主，从数据中发现入侵痕迹，对攻击行为进行预判、拦截。

4.4 中鸣网安加速中国网安在网站云防护和仿真靶场业务的布局

深圳市中鸣网安科技服务有限公司（简称"中鸣网安"）专注于新一代信息技术军民融合应用、网络信息安全、互联网文化产业三大核心领域。公司创始人及核心管理团队分别在 IT 行业教育培训、策划咨询、市场营销、信息技术应用、网络安全行业解决方案、网络研究、传媒产业等领域深耕多年，有望拓展中国网安安全系列产品的销售渠道，完善中国网安的理论、算法、芯片、产品、系统、服务的完整信息安全产业链布局。

中鸣网安热点产品有：

1）1-365GCD 网站安全防护服务

云防御平台涵盖智能 DNS 系统、云 WAF（WEB 防火墙）系统、缓存加速系统、日志存储及报表展现系统、运营管理系统（UI）、数据库/网站监控告警系统。

图 26：云防御平台

资料来源：公开网络，东兴证券研究所

2）安全运营服务

图 27：安全运营服务

环境及可靠性试验	高低温湿热试验、温度冲击试验、盐雾试验、淋雨试验、振动冲击试验、机械冲击试验、运输试验、三综合试验、离心加速度试验
电磁兼容检测服务	➢ 电磁兼容试验：CE101、CE102、CE107、CS101、CS106、CE106、CS103、CS104、CS105、CS109、CS114、CS115、CS116、RE101、RE102、RE103、RD101、RS105 ➢ EMC检测服务：10米法半波暗室、外场移动测试系统、电源测试系统等
软件测评	文档审查、代码审查、代码走查、功能测试、性能测试、接口测试、人机交互界面测试、边界测试、安装性测试
公共服务平台	移动互联网云测试服务、基础网络测试服务、信息系统测评服务、信息产品测试服务、安全服务、技术支持服务、人才培训服务、技术交流推广服务、政策性项目咨询及申报服务、宣传推广服务、资讯服务
工程教育	
仪器设备租赁维修	

资料来源：公开网络，东兴证券研究所

深圳中鸣网安是中国网安的全方位战略合作伙伴，是负责中国网安的网站云防护服务（“云防”）和禁卫靶场(“仿真靶场”)项目落地的全国运营机构。同时，代表中国网安与各地党政机关、企事业单位、行业单位积极融合合作，推动中国网安有关网络安全

产品、网络安全技术、网络安全行业解决方案服务及项目的落地，，在网站防护、检查、测试测评，网络安全人才培养，网络安全综合解决方案等服务方面做好政府的助手和智库。

4.4.1 网络云防护是政府和企业网站的迫切需要

如今网络安全问题日益突出，能否及时发现并成功阻止黑客的入侵和攻击、并保证互联网系统的安全

和正常运行已成为政府、企业等各类组织所面临的重要问题。特别是从当前信息安全攻击态势（主要特点：多点扫描攻击、利用最新漏洞 0day 攻击等）分析，原有传统的安全防御设施已无法适应新的安全需求。因此，利用新技术（云防护技术），增加安全防护层级，强化安全防护纵深，来加强防御多点扫描攻击、利用最新漏洞 0day 攻击等能力越来越迫切。

（1）云上应用安全需求

政府网站由于其承载着政府部门的重要业务，因此对 Web 应用防护有以下需求：

1）应用系统防护需求

云 WAF：为网站提供防攻击（跨站脚本攻击、注入攻击、缓冲区溢出攻击、Cookie 假冒、认证逃避、表单绕过、非法输入、强制访问）、防篡改（隐藏变量篡改、页面防篡改）、防 CC 攻击等安全防护。

网页防篡改：防止网站系统被黑客恶意攻击后篡改页面。

云安全检测：对云内业务信息系统进行全面的检测，需要覆盖可用性检测、木马检测、篡改检测、关键字检测，并定期进行漏洞扫描。

2）基于云的外部威胁感知需求

对于云计算环境下安全防护，仅做好内部的工作是不足的，因为外部威胁在持续演变，对外部威胁也必须保持足够的关注，因此对云外部威胁的感知对于云安全来说，也是必不可少的一部分。

3）云业务系统整体安全态势感知需求

不了解云端业务系统的整体安全态势，安全防护就是各种盲目地、漫无目的地措施集合，容易造成安全资源浪费，并且不利于安全事件发生后制定决策。而对云业务系统整体安全态势有了全面感知，则能根据获取到的各项信息进行综合分析，为云的安全防护制定更具针对性的措施。

（2）WEB 云防护技术

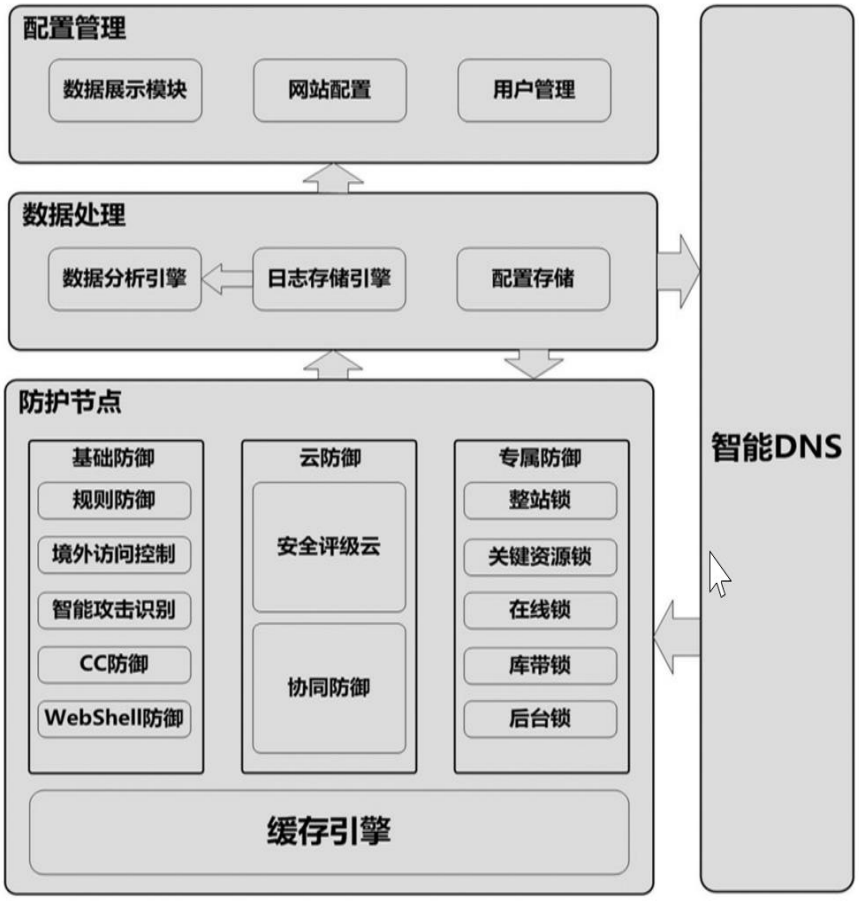
web 云防护技术是利用云计算技术和传统防御体系相结合，基于互联网方式，为目标网络提供安全检测、攻击过滤等服务的网络安全防护技术。从前海德沃网站可知，365GCD 网站安全防护服务的核心在于云防御平台和在线监测平台。

1）云防御平台：

云防御平台涵盖智能 DNS 系统、云 WAF（WEB 防火墙）系统、缓存加速系统、日志存储及报表展现系统、运营管理系统（UI）、数据库/网站监控告警系统。基于云防

御平台，在用户和网站之间构筑一道“无形”的防线，通过采用 Web 攻击智能识别，大规模网络访问日志的关联分析、黑客行为模式的特征收集，在互联网中进行流量数据的安全监测、大规模流量攻击分流、恶意行为拦截，保护 Web 网站的安全。

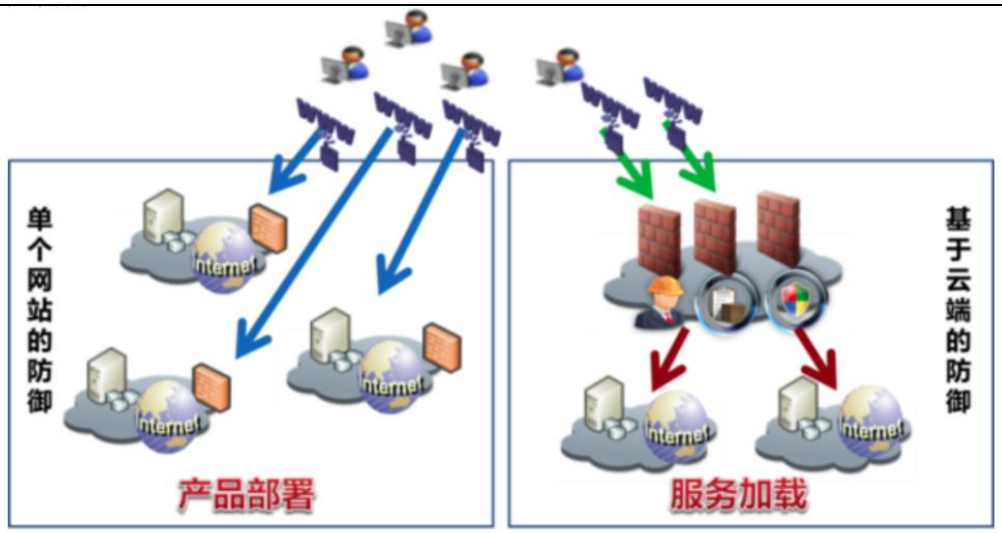
图 28：云防御平台



资料来源：公开网络，东兴证券研究所

与传统解决方案不同，云防御平台以服务加载的模式代替了产品部署的模式。过去对网站进行防护，需要在每个网站的互联网出口处部署 WAF 防火墙以抵御 Web 攻击的威胁。现在采用云安全服务的模式，在云防御平台上构筑虚拟防火墙。通过在网站侧加载服务，用户和网站之间的交互流量在云防御平台上进行过滤，从而达到防护网站的效果。

图 29：基于云端的防御和单个网站防御对比



资料来源：公开网络，东兴证券研究所

2）在线监测平台

网站在线监测平台主要由信息采集子系统（引擎系统）、分析研判子系统（数据存储中心和分析中心）、预警发布子系统（数据展现、态势感知、预警通知）、系统自维护和接口系统等组成。

图 30：网站在线监测平台

资料来源：公开网络，东兴证券研究所

基于网站在线监测平台开展面向网站的在线安全监测服务，可协助用户及时有效地了解网站是否安全可靠，网站是否存在恶意代码，网站是否运转正常，网站性能是否满足要求，并可对网站进行在线安全评估，同时采用灵活的告警方式，协助用户做到对网站状况了如指掌，快速的发现网站故障，减少损失和降低影响。

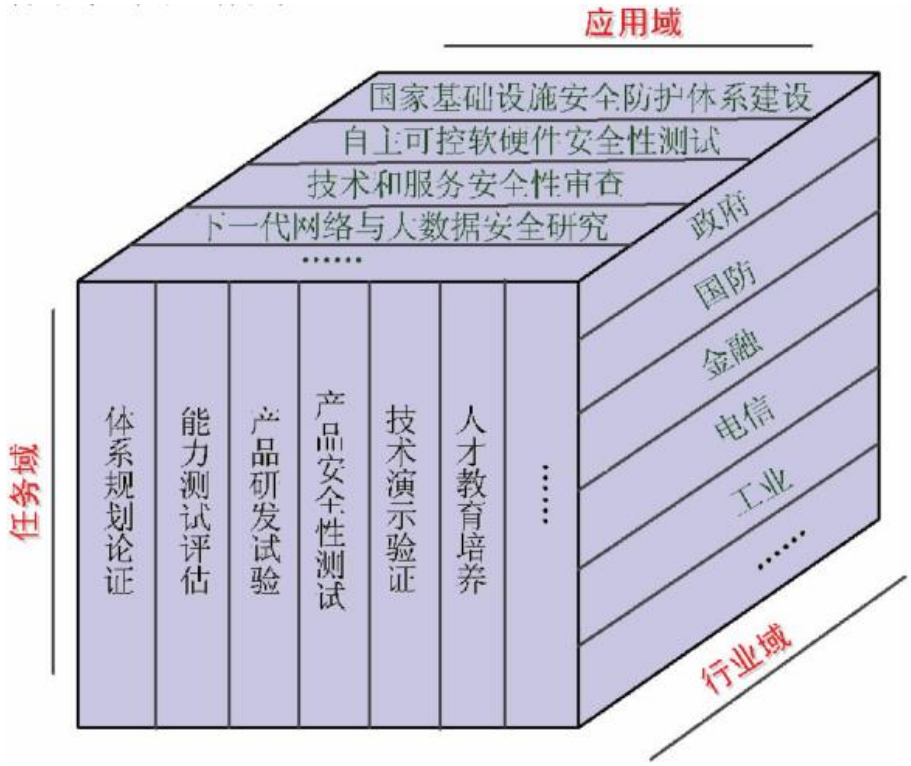
网站在线监测平台，对每个被监测的网站建立“健康”档案，在网站授权的条件下，定期收集网站的内容、状态、性能等相关信息进行分析和比对，以评估网站安全状况。

4.4.2 网络靶场是建设强大信息系统国度的安全保障

作为 2018 年国家网络平安宣传周的重头戏，“巅峰极客”网络平安技能挑战赛 19 天的报名时间内，共吸引了上万人报名。涵盖国家关键信息基础设施单位、自主可控厂商、互联网企业、渗透测试团队、知名院校及个人。其中亮点是决赛首次采用城市网络平安仿真靶场，让战队分别扮演攻击、防御、公共网络执法等不同角色，展现一个城市遭遇网络攻击之后可能诱发的种种社会问题。

网络靶场一般是针对网络攻防演练和网络新技术评测的重要基础设施，主要供政府、军队、企业等使用，用来提高网络和信息系统的稳定性、安全性等性能。在军事应用方面，网络靶场是为适应军事领域内信息系统和信息化武器装备的发展要求，提供近似实战的信息战环境而建立的网络安全试验平台。网络靶场可以为各种网络技术、攻击防御手段以及安全性策略和方案提供定量和定性的评估，实现信息系统和信息化武器装备的技战术性能测试和作战效能评估，为信息安全主管机构评估网络信息系统的安全程度提供一个可信性、可控性、可操作性强的试验环境。

图 31：国家网络靶场概念



资料来源：公开网络，东兴证券研究所

网络靶场的主要功能包括:(1)网络攻防武器评测验证:新型网络攻防武器研制出来之后,需要对其进行测试验证,是否能有效攻破敌方防护系统,以及是否能有效保护我方目标系统;2)支持人员培训与竞演:随着新型网络攻防武器的研发,具体网络安全人员能否能有效掌握,训练后,谁掌握的技能更好;3)科学试验和新技术验证:网络空间科研人员研制出新的网络协议,新型网络设备,以及不同网络新技术,在互联网上功能和性能如何,也需要进行验证。

（1）国外靶场发展历程

网络靶场的发展可以分为三个阶段：

第一阶段是以 21 世纪初期针对单独的木马类攻击武器而建立的实物高逼真型靶标时期。

在此阶段,各国以敌方的靶标软硬件平台为目标,建立尽可能逼真的靶标软硬件平台,用于测试己方新研制的攻击武器能否成功绕过敌方的防护软件,主要包括早期的蜜罐系统、木马测试系统等。

第二阶段是以 2005 年开始的小型虚拟化互联网靶场时期。

在此阶段,云计算、软件定义网络等虚拟技术是该阶段的主流技术,模拟真实的互联网攻防作战提供虚拟环境是各个国家的主要目标,但模拟的互联网规模都比较小。主要包括:2005 年美军联合参谋部组织建设的“联合信息作战靶场”(IOR),2009 年美国国防部国防高级研究计划局牵头建立的“国家网络靶场”(NCR),2010 年美军国防信息系统局组织建设的“国防部网络安全靶场”(GIG);2010 年英国国防部正式启用了由诺•格公司研制的“网络安全试验靶场”;此外,日本的 StarBed 靶场系统,加拿大的 CASELab 靶场系统,英国的 SATURN 靶场系统以及台湾的 Testbed 测试平台等均属于这一阶段。

第三阶段是 2014 年开始的支撑泛在网的大型虚实结合网络空间靶场时期。

在此阶段,“震网”、“火焰”等针对工控网的新型网络攻击突现,各国纷纷开始研究虚实结合的网络空间靶场技术。主要包括:2014 年美国国家靶场增加了法拉第罩进行无线发射设备的测试,并支持移动计算设备;2014 年 6 月,北大西洋公约组织在塔林建立 NATO 的网络靶场,支持工控网的攻防测试;2015 年 7 月,欧洲防务署批准建立网络攻防测试靶场,标志着 EDA 靶场工程的启动。

（2）现存网络靶场体系

现有靶场主流体系架构主要有美国的 Emulab,DeterLab,英国的 breakingPoint 靶场,日本的 Starbed 靶场,美国 NCR 靶场等。

图 32：网络靶场体系架构对比

体系 / 技术	EmuLab[5]	BreakingPoint[7]	Starbed[8]	NCR[9]	基于 IaaS 大的 NCR[13]	xCloudbed
1 基础平台技术	分布式集群 + 虚拟化	集群 + 虚拟化	集群	集群 + 虚拟化	IaaS 云平台技术、SDN 技术	云及虚拟化
2 试验过程控制技术						
拓扑设计	NS 脚本、Web 可视化拓扑设计	Web 可视化拓扑设计	Web 可视化拓扑设计	Web 可视化拓扑设计	Web 可视化拓扑设计	Web 可视化拓扑设计
节点虚拟化	Virtual PC	KVM	不支持	KVM	KVM	KVM、Docker
链路虚拟化	Dummynet	Linux bridge	Linux bridge	Linux bridge	OVS	OVS
系统互联	bridge	bridge	bridge	bridge	OVS	OVS
数据采集	带内	带内	带内	带内	带内	带外
结果评估	支持	支持	支持	支持	支持	支持
3 系统特点						
优点	支持物理机及网络接入,虚拟网络互联,脚本可编程性好	支持物理机及网络接入,虚拟网络互联	速度快,制行效率高	支持物理机及网络接入,虚拟网络互联	支持物理机及网络接入,虚拟网络互联	支持物理机及网络接入,虚拟网络互联
缺点	混合架构,存在兼容性问题	混合架构,存在兼容性问题	动态扩展性差	混合架构,存在兼容性问题		

资料来源：公开网络，东兴证券研究所

（3）美军网络靶场现状

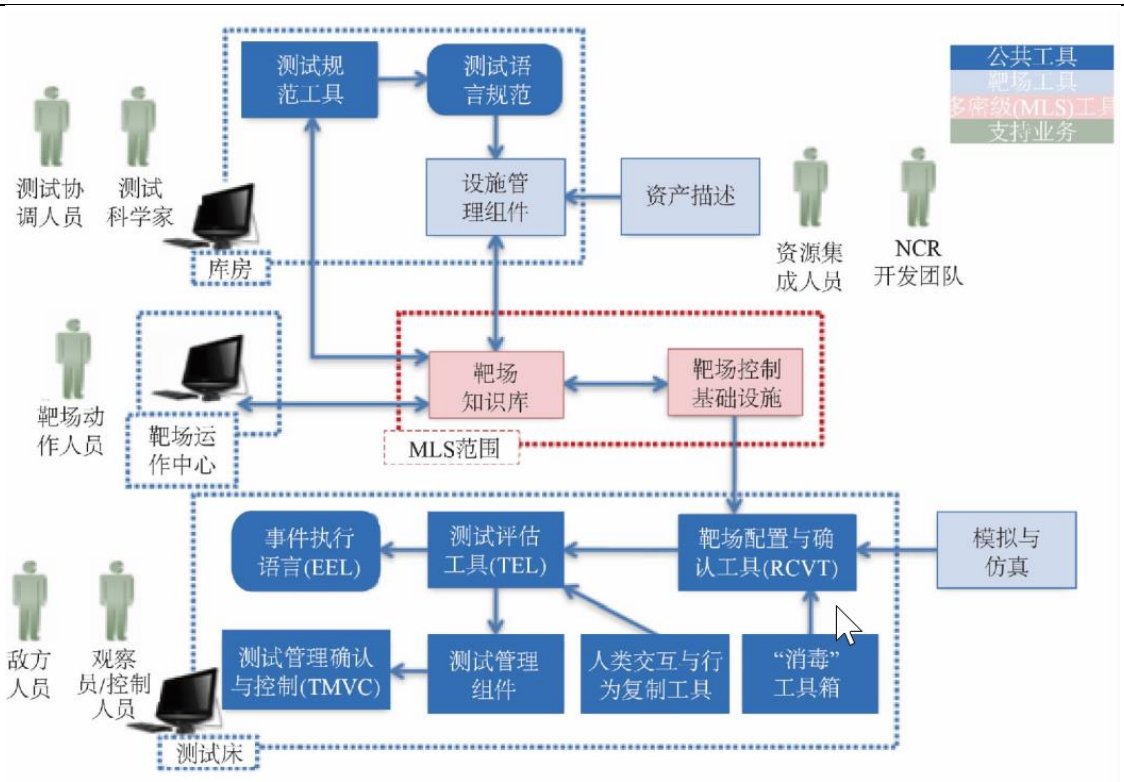
在网络靶场建设方面,美国走在了世界的前列,除了建成多个小型网络靶场外,已开展国家级的网络靶场建设。

2008 年 1 月 8 日，美国时任总统布什签署“国家网络安全综合计划（Comprehensive National Cyber Security Initiative，CNCI）”，“国家网络靶场（National Network Range，NCR）”是该项目的重要组成部分。项目由国防部先进研究项目局（Defense Advanced Research Projects Agency，DARPA）”负责管理，靶场建成后将为美国国防部、陆海空三军和其他政府机构服务。NCR 项目是美国国会向 DARPA 直接下达的 70 年来的唯一项目。

NCR 项目的参与方包括信息安全企业、学术机构和商业实体，包括 BAE 系统公司、通用动力公司、约翰霍普金斯大学应用科学实验室、洛克希德·马丁公司、诺斯洛普·格鲁门公司、应用科学国际集团和斯巴达公司。

构建 NCR 的目标为：以真实的网络作战环境为模拟对象，以各种网络、电子战手段为技术对抗对象，通过模拟真实环境的演练实现网络战实力的大幅提升，在网络战争时期能够确保打赢。

图 33：赛博靶场原型系统体系结构



资料来源：公开网络，东兴证券研究所

NCR 建成后，可以达到在 15 分钟内重新组建试验节点，在 1 小时内重新配置靶场，在 2 小时内进行 10000 个节点试验的工作效率。获得政府授权的测试组织可与 NCR 执行机构协调，安排靶场资源与时间。测试过程主要分为三个阶段。首先，在测试开

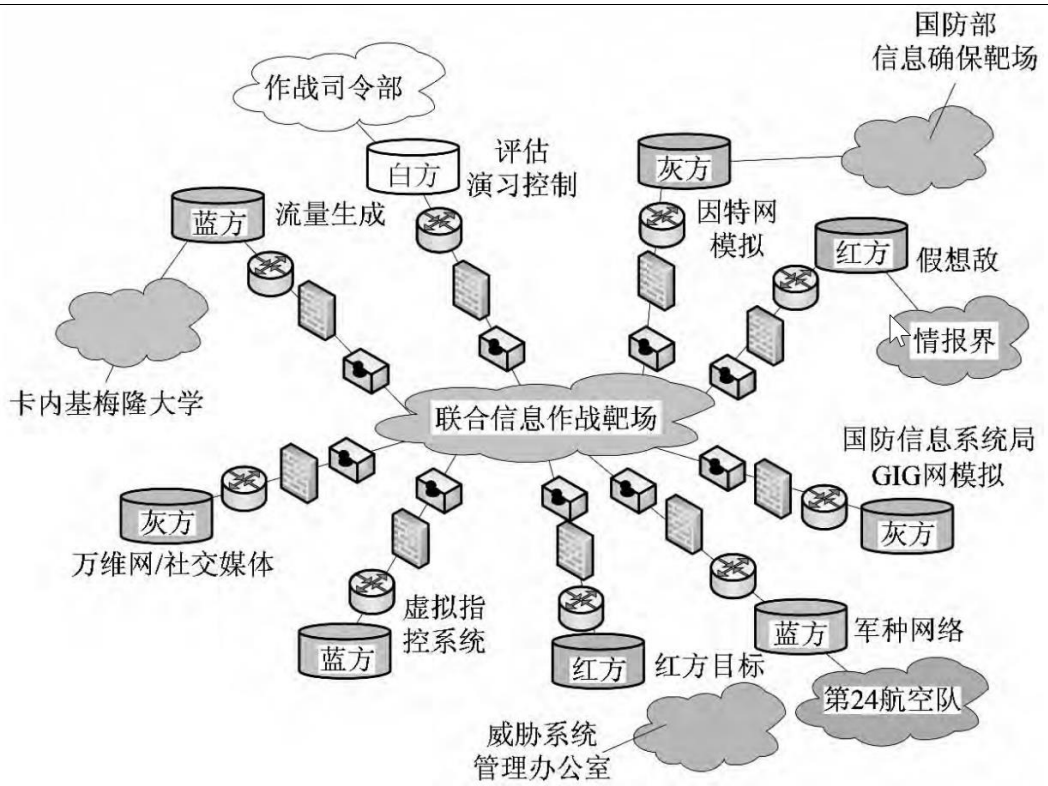
始之前，NCR 工作人员将使用 CSTL 测试规范工具构建测试平台，构建过程包括对测试平台进行分区，为测试分配系统资源，以及集成和配置共同的硬件 / 软件资源和网络工具，作为测试的资产描述。其次，通过 NCR 的数据传感器、资源管理器、范围存储库和可视化工具进行收集客户指定的事件数据。在这个过程中，范围配置以及验证工具会自动将硬件连接到适当的配置并且自动配置所需要运行的软件。最后，使用测试执行工具、流量生成工具以及特定系统执行测试队列，进行数据收集以及分析。

NCR 关键技术：

NCR 与传统的电子靶场、通信靶场之间存在较大差异，主要表现在靶场的试验规模、对象、环境、安全与复杂度等方面。NCR 在建设中面临许多关键技术和难点，主要包括大规模网络仿真环境构建技术、靶场试验时钟同步技术和靶场试验运行控制技术等。

除了众所周知的国家赛博靶场(NCR)外，美军还陆续启动了国防部信息确保靶场(DoDIAR)、联合赛博空间作战靶场(JCOR)、海军赛博空间作战靶场(NCOR)、联合信息作战靶场(JIOR)、战略司令部赛博作战靶场(SCOR)等。

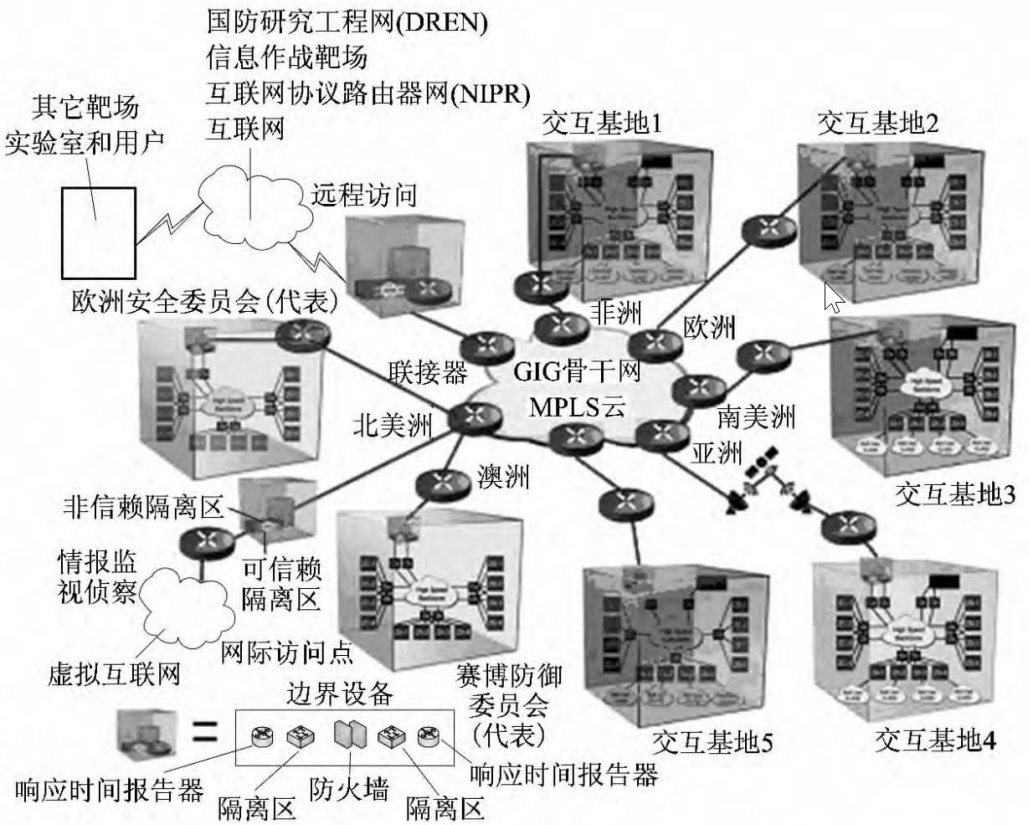
图 34：联合信息作战靶场典型试验体系结构



资料来源：公开网络，东兴证券研究所

国防部信息确保靶场这一赛博空间“沙盘”可以模拟全球信息栅格(GIG)，进行赛博试验鉴定和训练演练。靶场可以用作独立的模拟器，也可以与各作战司令部、各军种和国防部各机构的其他靶场连接和互操作。

图 35：GIG 与其他靶场连接和互操作



资料来源：公开网络，东兴证券研究所

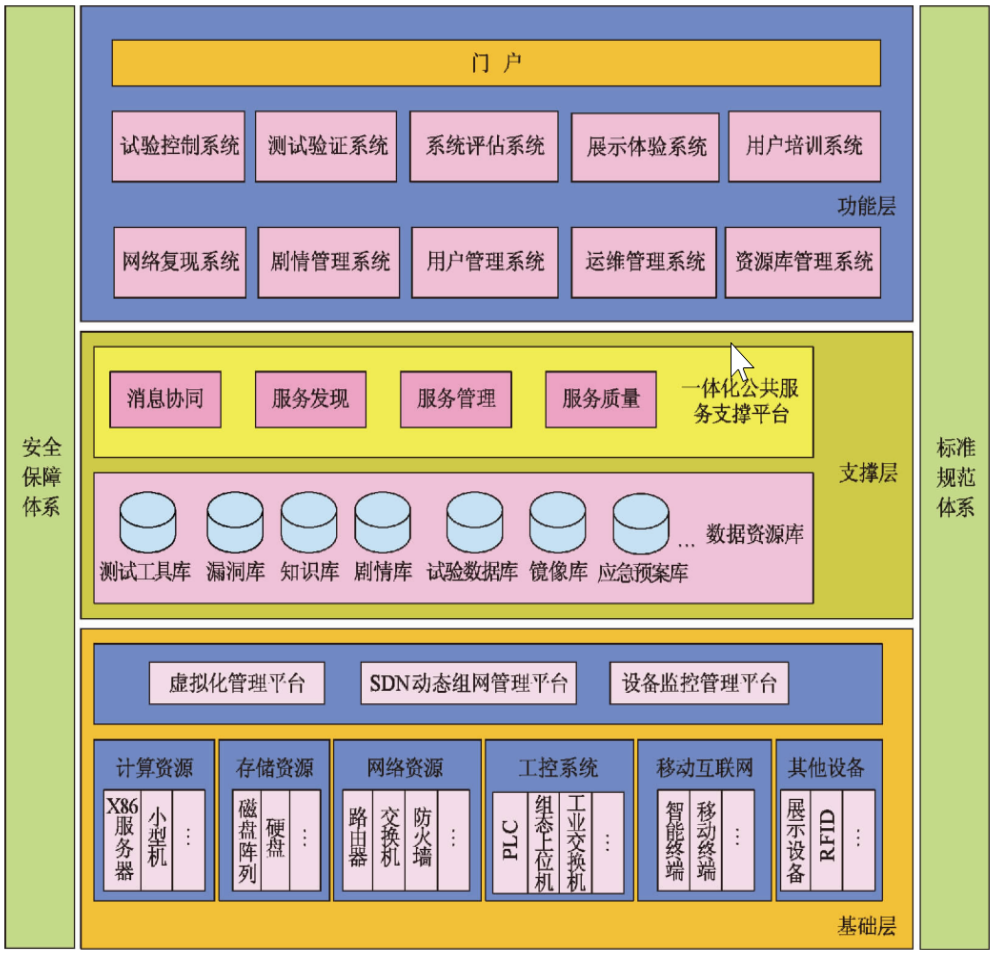
4.4.3 网络安全总体靶场我国仍有不小差距

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，我国都还存在着不小的差距。国家网络靶场建设是国家网络空间安全战略的迫切需要，是提升我国网络空间安全能力的重要战略举措，是建设强大信息系统国度的安全保障。

通过国家网络靶场建设，可为金融、电信、能源、交通、电力等国家关键信息基础设施安全体系建设提供分析、设计、研发、集成、测试、评估、运维等全生命周期保障服务，解决无法在真实环境中对复杂大规模异构网络和用户进行逼真的模拟和测试，以及风险评估等问题，实现国家网络空间安全能力的整体跃升。

国家网络靶场体系结构设想如图所示，主要包括靶场基础环境、数据资源库、服务支撑、靶场应用、标准规范体系和安全保障体系。

图 36：国家网络靶场体系架构



资料来源：公开网络，东兴证券研究所

5. 卫士通背靠中国网安集团资源，肩负信息安全国家队职责

卫士通公司一直切实肩负起“信息安全国家队”的使命责任，致力打造从芯片到系统的全生命周期安全解决方案，为党政军用户、企业级用户和消费者提供专业自主的网络信息安全解决方案、产品和服务。

图 37：卫士通发展动能

资料来源：公开网络，东兴证券研究所

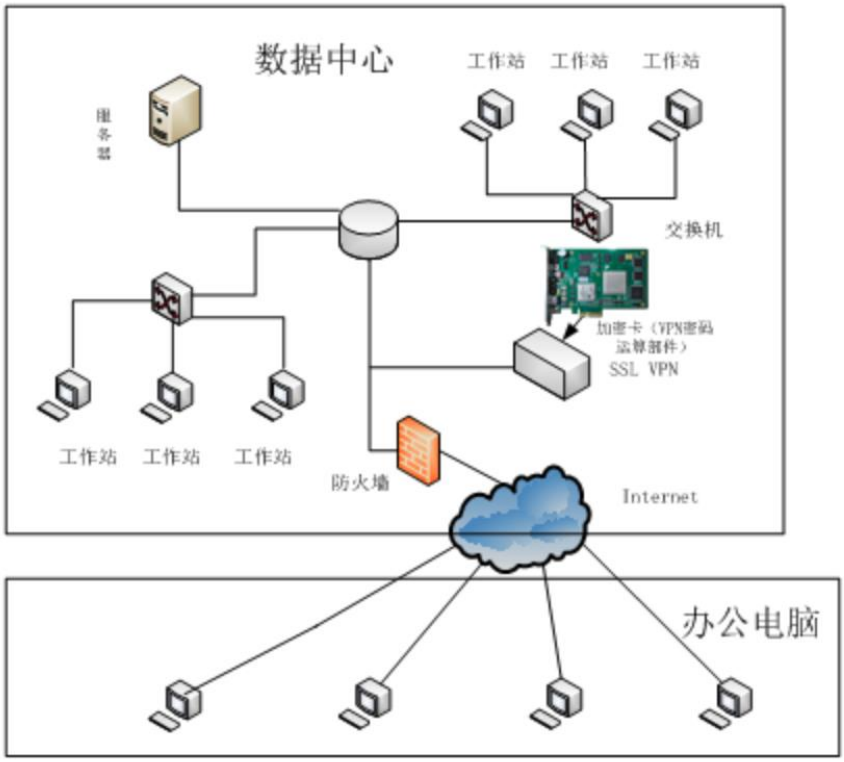
5.1 公司密码产品

图 38：公司密码产品

资料来源：公开网络，东兴证券研究所

1）密码芯片&密码卡：密码卡能为系统提供数字签名/验证、数据加密/解密和信息完整性保护，同时也能为访问用户提供身份鉴别功能。

图 39：密码卡应用



资料来源：公开网络，东兴证券研究所

2）密码模块：智能密码钥匙芯片和读卡器于一体，采用软件与硬件结合设计，可以为终端计算机提供认证、签名验证、加密解密、消息摘要等安全密码服务，保证了用户数据的机密性、真实性和完整性。

图 40：智能密码钥匙

资料来源：公开网络，东兴证券研究所

智能密码钥匙适用于安全防护或认证相关系统的多种终端，例如，卫士通终端安全登录与文件保护系统、卫士通安全网关、电子文档公文系统等。

图 41：智能密码钥匙技术指标简介

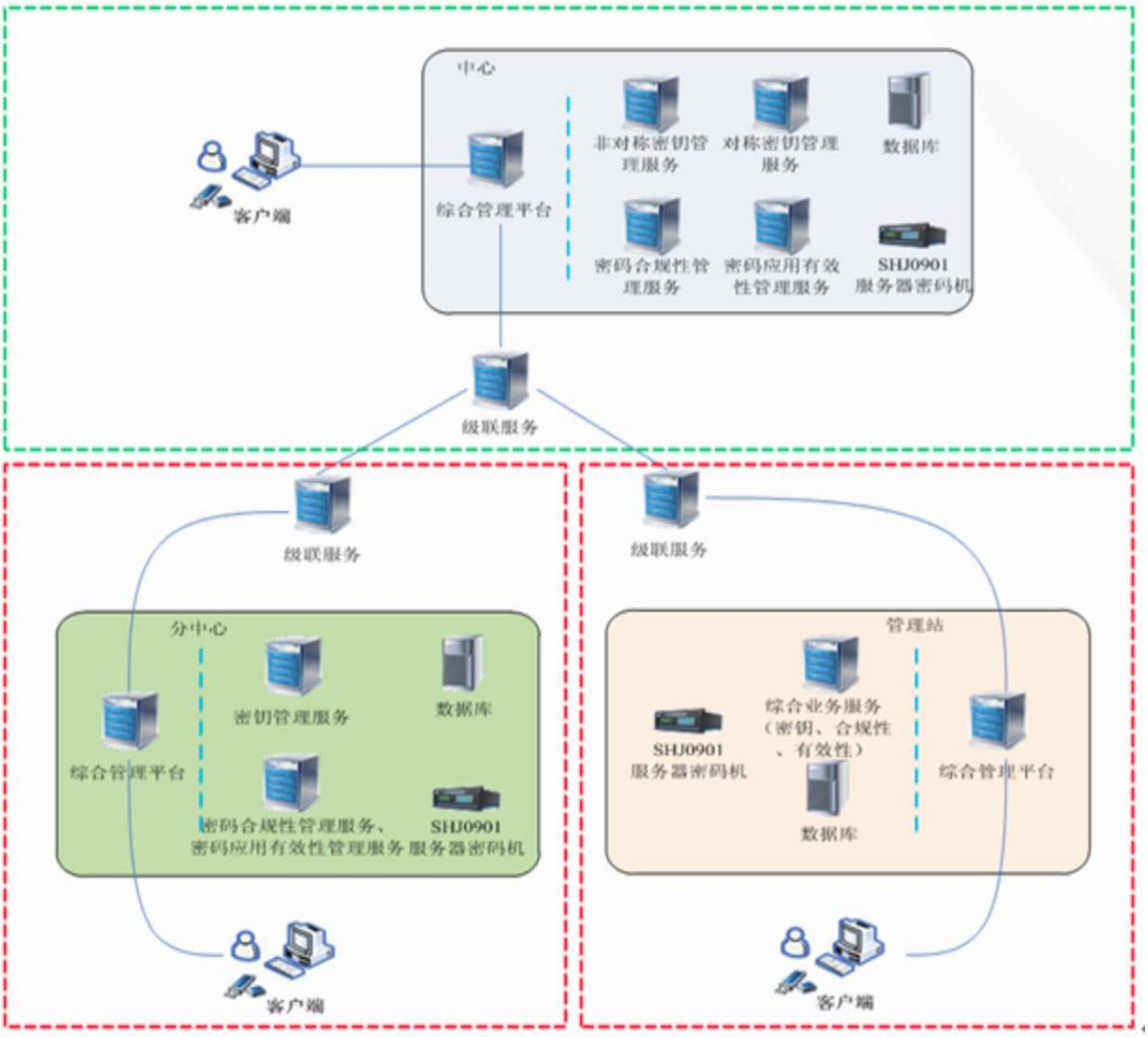
技术指标			智能密码钥匙 DTE256-USBKEY	智能密码钥匙 DTE256H-USBKEY	智能密码钥匙 HTE256-USBKEY	智能密码钥匙 HTE256H-USBKEY
支持的接口			1. 支持标准 CSP 2. 支持标准的以及自定义商密扩展的 PKCS#11	1. 支持标准 CSP 2. 支持标准的以及自定义商密扩展的 PKCS#11	1. 支持标准 CSP 2. 支持标准的以及自定义商密扩展的 PKCS#11 3. 支持国密接口，并可与扩展 CSP 相通	1. 支持标准 CSP 2. 支持标准的以及自定义商密扩展的 PKCS#11 3. 支持国密接口，并可与扩展 CSP 相通
驱动模式			低功耗，智能卡驱动和专用驱动两种驱动模式	低功耗，智能卡驱动和专用驱动两种驱动模式	低功耗，智能卡驱动	低功耗，智能卡驱动
运行环境	操作系统环境	Windows 系列	xp/2003/7/2008/8 (32 位与 64 位)	xp/2003/7/2008/8/10 (32 位与 64 位)	xp/2003(32 位)、Win7/2008 (32 位与 64 位)、Win8(32 位)	xp/2003/7/2008/8/10 (32 位与 64 位)
		国产操作系统	中标麒麟、普华	中标麒麟、普华	中标麒麟、普华	-
		通用	Redhat、Fedora、CentOs、Ubuntu 等（可定制）	Redhat、Fedora、CentOs、Ubuntu 等（可定制）	Redhat、Fedora、CentOs、Ubuntu 等（可定制）	-
	支持的硬件平台		arm64/mips/x86/sparc32，其他平台可定制	arm64/mips/x86/sparc32，其他平台可定制	arm64/mips/x86/sparc32，其他平台可定制	-

资料来源：公开网络，东兴证券研究所

3）密码系统：也分为多种，密码管理系统，数字证书认证系统，云密码管理系统。

以密码管理系统为例，密钥管理系统（SYT1209）是一款符合国家密码管理局相关标准和规范，并参考国家相关职能部门指导意见，整体规划和设计的密钥管理类产品。系统以密码技术为核心基础，利用密码技术保障密钥全生命周期的安全。系统可广泛应用于电子政务外网、电力等领域，为信息化系统建立完整的密钥管理体系，满足以对称密钥体系和非对称密钥体系为主的密钥管理服务需求。密钥管理系统支持单级模式和级联模式，可以根据实际的应用环境及需求进行系统级联配置。级联配置成功后，系统将分为中心和分中心两级，中心和分中心之间的数据通讯均由级联服务提供传输通道和加密保护。

图 42：密码管理系统



资料来源：公开网络，东兴证券研究所

4）服务器密码机：具有数据加解密、签名、验签、MAC、杂凑等功能，可为用户解决敏感信息机密性、完整性、有效性和不可抵赖等安全性问题。

服务器密码机作为商用基础密码产品，它既可以为信息安全传输系统提供高性能的数据加/解密服务，又可以作为主机数据安全存储系统、身份认证系统以及对称、非对称密钥管理系统的主要密码设备和核心构件，具有广泛的系统应用潜力。可广泛应用在银行、保险、证券、交通、邮政、电子商务、移动通信等行业的安全业务应用系统中。

5.2 信息安全产品

图 43：信息安全产品

资料来源：公开网络，东兴证券研究所

5.3 安全信息产品

图 44：安全信息产品

资料来源：公开网络，东兴证券研究所

5.4 公司客户

经过二十年的市场实践，卫士通公司以优秀卓越的服务能力，为国家政府部委、涉及国计民生的金融行业、能源行业以及军工行业和通信运营企业提供了高质量、全方位的信息安全服务，并在业内积累了良好口碑。

图 45：公司主要客户

政府部委

全国人民代表大会 The National People's Congress of the People's Republic of China
中共中央纪律检查委员会
中华人民共和国国家监察委员会
中华人民共和国最高人民检察院 The Supreme People's Procuratorate of the People's Republic of China
中华人民共和国最高人民法院 The Supreme People's Court of The People's Republic of China
中华人民共和国国家发展和改革委员会 National Development and Reform Commission
中华人民共和国财政部 Ministry of Finance of the People's Republic of China
中国证券监督管理委员会 CHINA SECURITIES REGULATORY COMMISSION
中国科学院 CHINESE ACADEMY OF SCIENCES
国家海洋局 State Oceanic Administration, People's Republic of China
....

金融行业

中国人民银行
中国银联 China Unionpay
国家开发银行 CHINA DEVELOPMENT BANK
中国进出口银行 THE EXPORT-IMPORT BANK OF CHINA
ICBC 中国工商银行
中国农业银行 AGRICULTURAL BANK OF CHINA
中国银行 BANK OF CHINA
中国建设银行 China Construction Bank
交通银行 BANK OF COMMUNICATIONS
Bank 中国光大银行 共享阳光·创新生活
CITIC 中信银行
招商银行 CHINA MERCHANTS BANK
HUAXIA BANK 华夏银行
....

能源行业

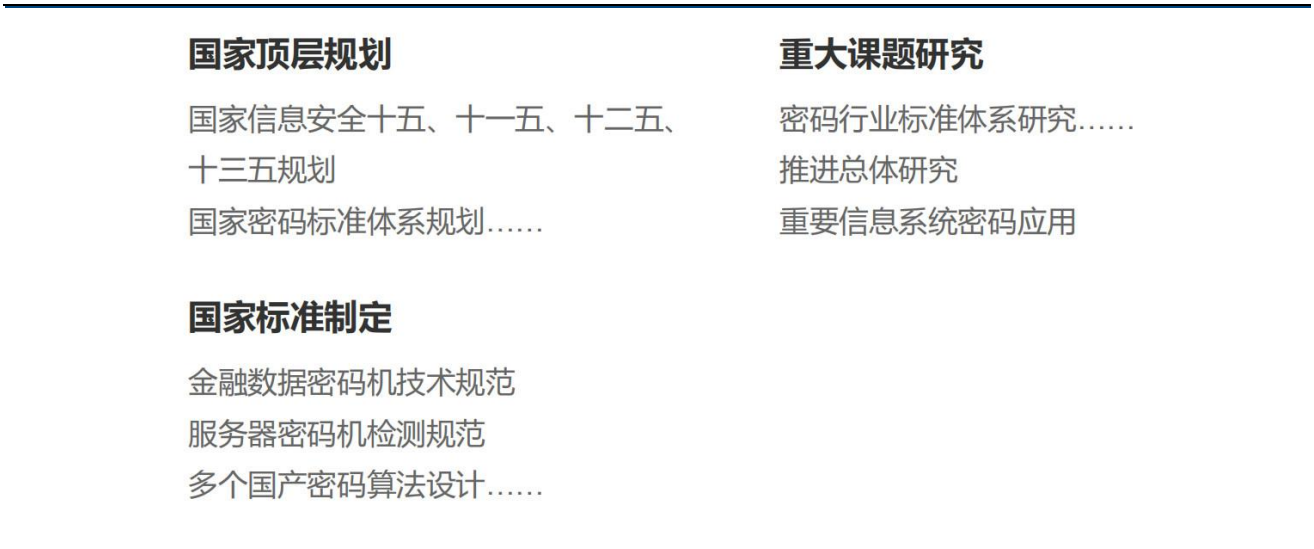
国家能源集团 CHN ENERGY
国家电网 STATE GRID
中国南方电网 CHINA SOUTHERN POWER GRID
中国石油
中国石化 SINOPEC
中国国电 CHINA GUODIAN
国家电投
中国华能 CHINA HUANENG
中国华电 CHINA HUADIAN
中国长江电力股份有限公司 China Yangtze Power Co.,Ltd.
....

资料来源：公开网络，东兴证券研究所

5.5 参与了多个国家信息安全蓝图设计，承担和参与多个国家前沿科技创新项目

卫士通公司是国内少数具有完备信息安全设备生产和研发资质的企业，通过过硬的技术和创新实力主导和参与了多个国家信息安全蓝图设计，承担和参与多个国家前沿科技创新项目，并在国家重大事件和活动中积极发挥“大国重器”的责任使命。

图 46：参与国家信息安全蓝图设计

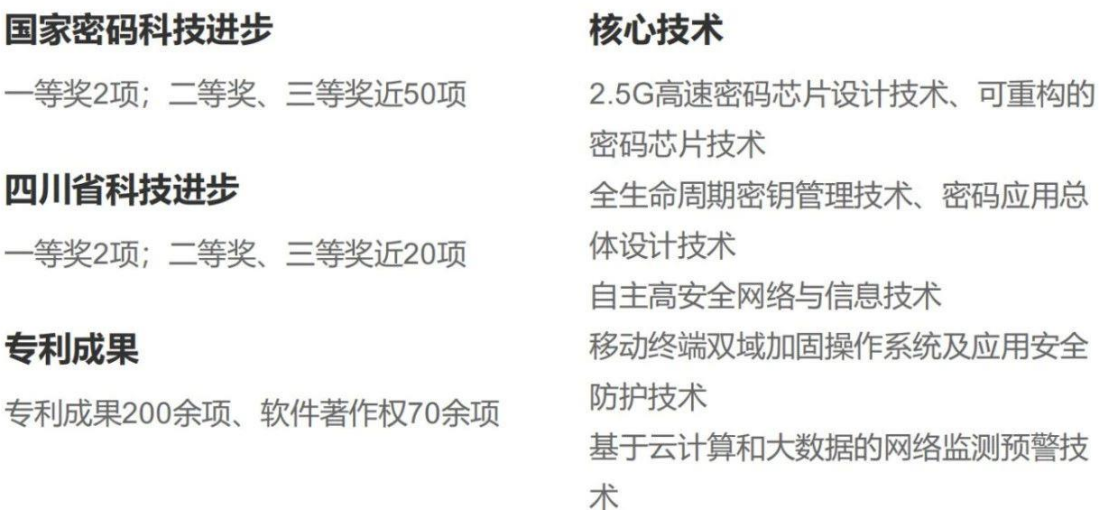


资料来源：网络资料，东兴证券研究所

图 47：承担大量国家科研创新项目

资料来源：网络资料，东兴证券研究所

图 48：引领信息安全核心技术发展



资料来源：网络资料，东兴证券研究所

5.6 渠道布局深入，人才队伍专业

卫士通公司率先在业内完成全国化业务布局，建立了以成都为管理总部、北京为营销总部的双总部体系，建成了覆盖全国的 6 大区域营销中心，以及 25 家办事处，可在更短时间内为全国范围的用户提供本地化的营销和服务体验。

图 49：全国化业务布局

资料来源：网络资料，东兴证券研究所

卫士通公司拥有高素质的专业人才队伍，建有人力资源和社会保障部定点博士后工作站，现有员工超过 2000 人，技术人员占比超过 66%，博士及业界专家 60 余人，硕士研究生及以上学历占比超过 30%。

图 50：高素质专业人才队伍

资料来源：网络资料，东兴证券研究所

随着保密工作重要性愈发突出，信息安全自主可控是我国保密工作的重中之重。中鸣网安负责中国网安的网站云防护服务（“云防”）和禁卫靶场(“仿真靶场”)项目落地，中国网安构建包括理论、算法、芯片、产品、系统、服务在内的完整信息安全产业链战略得以实现。中国网安旗下唯一上市公司卫士通有望借助中鸣网安渠道打开局面，利用自身央企安全运维、云安全、保密终端、密码产品等方面优势，继续拓展自身在央企信息安全领域优势，打造央企综合信息安全应用体系。

6. 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 27.15 亿元、52.27 亿元和 76.92 亿元，归母净利润分别为 1.60 亿元、5.47 亿元和 8.08 亿元，EPS 分别为 0.19 元、0.65 元和 0.96 元，维持公司“强烈推荐”评级。

7. 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 3：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	2140	4067	5156	9778	14339	**营业收入**	1799	2137	2715	5227	7692
货币资金	524	1881	2389	4600	6769	**营业成本**	1165	1383	1776	3054	4393
应收账款	1088	1616	2053	3953	5817	营业税金及附加	15	20	9	17	25
其他应收款	59	67	85	163	240	营业费用	177	215	285	549	808
预付款项	55	68	85	114	156	管理费用	271	330	421	810	1192
存货	193	211	271	466	670	财务费用	6	-12	-9	80	232
其他流动资产	29	25	20	-5	-29	资产减值损失	47.47	74.60	74.60	74.60	74.60
非流动资产合计	1509	1686	1464	1300	1137	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	27	27	27	27	投资净收益	1.87	1.80	1.80	1.80	1.80
固定资产	268.05	265.66	1270.43	1113.41	956.39	**营业利润**	120	153	161	644	970
无形资产	10	71	63	57	51	营业外收入	76.69	50.75	50.75	50.75	50.75
其他非流动资产	0	55	55	55	55	营业外支出	0.16	0.74	0.74	0.74	0.74
资产总计	3649	5754	6620	11078	15477	**利润总额**	196	203	211	694	1020
流动负债合计	2026	1309	2057	6128	9961	所得税	23	26	42	139	204
短期借款	829	0	398	3440	6174	**净利润**	173	177	169	556	816
应付账款	759	980	1242	2136	3072	少数股东损益	17	8	8	8	8
预收款项	40	60	84	131	201	归属母公司净利润	156	169	160	547	808
一年内到期的非	0	0	0	0	0	EBITDA	161	238	315	888	1364
非流动负债合计	50	57	57	57	57	**EPS（元）**	0.36	0.21	0.19	0.65	0.96
长期借款	0	0	0	0	0	**主要财务比率**					
应付债券	0	0	0	0	0		2016A	2017A	2018E	2019E	2020E
负债合计	2077	1366	2113	6185	10018	**成长能力**					
少数股东权益	84	92	100	108	117	营业收入增长	12.21%	18.80%	27.05%	92.51%	47.16%
实收资本（或股	433	838	838	838	838	营业利润增长	-9.33%	28.11%	4.89%	301.18%	50.54%
资本公积	300	2558	2558	2558	2558	归属于母公司净利润	4.69%	8.54%	-5.18%	241.42%	47.61%
未分配利润	708	848	910	1121	1432	**获利能力**					
归属母公司股东	1489	4296	4406	4784	5342	毛利率(%)	34.57%	41.58%	42.89%	42.30%	43.14%
负债和所有者权	3649	5754	6620	11078	15477	净利率(%)	9.61%	8.29%	6.21%	10.63%	10.61%
现金流量表					单位:百万元	总资产净利润（%）		4.27%	2.94%	2.42%	4.94%
	2016A	2017A	2018E	2019E	2020E	ROE(%)	10.46%	3.94%	3.64%	11.44%	15.12%
经营活动现金流	-137	-51	165	-509	-10	**偿债能力**					
净利润	173	177	169	556	816	资产负债率(%)	57%	24%	32%	56%	65%
折旧摊销	35.55	97.30	0.00	157.02	157.02	流动比率	1.06	3.11	2.51	1.60	1.44
财务费用	6	-12	-9	80	232	速动比率	0.96	2.95	2.38	1.52	1.37
应收账款减少	0	0	-437	-1899	-1864	**营运能力**					
预收帐款增加	0	0	24	47	69	总资产周转率	0.57	0.45	0.44	0.59	0.58
投资活动现金流	-634	-181	-14	-73	-73	应收账款周转率	2	2	1	2	2
公允价值变动收	0	0	0	0	0	应付账款周转率	2.59	2.46	2.44	3.09	2.95
长期股权投资减	0	0	0	0	0	**每股指标（元）**					
投资收益	2	2	2	2	2	每股收益(最新摊薄)	0.36	0.21	0.19	0.65	0.96
筹资活动现金流	733	1579	358	2793	2252	每股净现金流(最新	-0.09	1.61	0.61	2.64	2.59
应付债券增加	0	0	0	0	0	每股净资产(最新摊	3.44	5.12	5.26	5.71	6.37
长期借款增加	0	0	0	0	0	**估值比率**					
普通股增加	0	406	0	0	0	P/E	53.99	92.18	101.66	29.78	20.17
资本公积增加	6	2258	0	0	0	P/B	5.65	3.79	3.70	3.41	3.05
现金净增加额	-38	1347	509	2210	2169	EV/EBITDA	54.24	60.51	45.37	17.05	11.51

资料来源：东兴证券研究所

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。