东兴证券 DONGXING SECURITIES

对标美国 FireEye 追求网络攻防绝对优势

——卫士通（002268）深度报告系列之四

2019 年 02 月 17 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

报告摘要：

中美网络攻防能力差距较大，政策战略加快部署利好网络安全行业。全球网络空间呈现对抗公开化、力量专业化、部署攻势化的趋势。网络安全攻防、防御成本急剧上升，碎片化安全问题严重，国际网络空间竞争博弈进入深水区。美国国家级攻防对抗将成为新常态，我国网络安全面临高压态势。我国网络空间防御能力严重滞后，国内网络安全行业有望进一步整合发展。

美国火眼公司（FireEye）并购建立综合安全管理平台，军民融合、政企合作具有借鉴意义。美国火眼公司在 APT 防御、网络安全服务生态系统领域独步武林，通过并购实现在安全服务领域较大的跨越，搭建起了以侦测、响应、情报、咨询为一体的综合安全管理平台，主业逐渐向服务类转向。而火眼自 2013 年后收入增长了八倍，给卫士通未来发展指明了道路，向服务转型，通过收购建立生态系统将是卫士通未来发展的两道法门。

网络安全行业加速增长，行业技术发展催生更大市场需求，业务模式转向运维。数据资产急速增长，传统边界安全转向内容安全和数据安全；云安全带来虚拟化需求，成为云-网-端立体式安全核心；物联网安全和工控安全兴起、5G 部署将进一步扩大网络攻击范围，催生新的防御需求。

随着等保 2.0 的临近，网络安全产业市场空间进一步增加，网络安全行业整合趋势进一步增强，中美贸易冲突下国家队将充分受益，**重点推荐卫士通（002268）。**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,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。

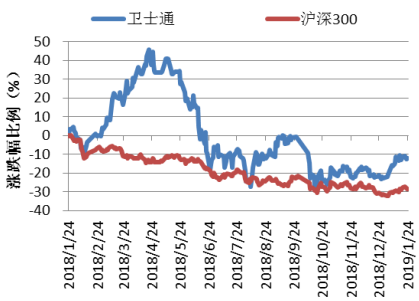
财务指标预测

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

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

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

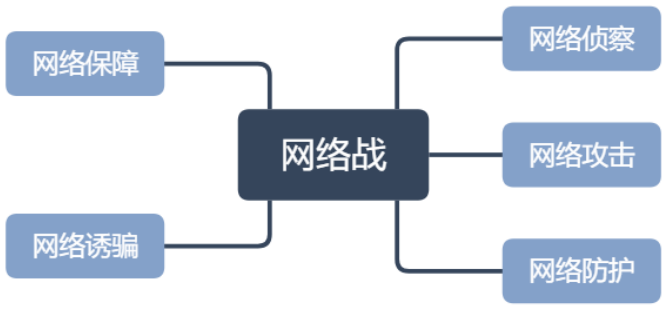
1. 网络战成为当前国家之间对抗的重要组成部分

1.1 网络攻防——新冷战下的对抗神器

网络战是信息战的通常形式，是指敌对各方在政治、经济、军事等领域，为争夺和达成信息优势，掌握并确保网络空间信息权，利用网络技术在保证自身信息和网络系统安全的基础上，扰乱、破坏敌方网络和信息系统的作战形式。这种全新的作战行动样式，包括网络侦察、网络攻击、网络防护、网络诱骗、网络保障等。随着网络攻击手段的不断完善，其投送方式已由人工投送发展为无线电信号和激光信号投送，使**网络攻击行动更加隐蔽，破坏性不断增大，网络攻防更加激烈。因具有隐蔽性、安全性、不易追溯性的特点，为新冷战情绪下的新型兵种。**

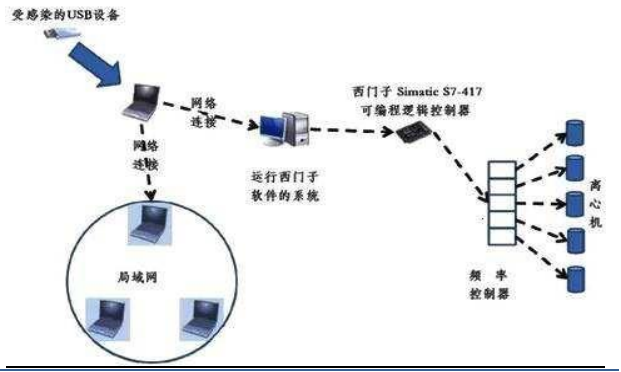
作为与陆海空天并列的人类活动“第五空间”，网络已成为维护国家安全和打赢现代战争的必争之地。近年来，全球网络空间呈现对抗公开化、力量专业化、部署攻势化的趋势，以战略网络战为代表的网络空间军事手段异军突起。当前，网络空间对实体空间的加速覆盖和深度融合，以及网络武器的实战化和多样化，都在不断催化战略网络战向具体行动样式裂变繁衍，军事强国基于网络空间实施阻流瘫点、制权毁体、攻心控局正在成为现实。当前，越来越多的国家开始把网络空间列为未来重要的国防空间。俄罗斯对爱沙尼亚、格鲁吉亚等国发动的大规模网络战；美国、以色列对伊朗核设施发动的“震网”病毒攻击；“阿拉伯之春”中网络社交工具的推波助澜作用。对网络空间成功实施攻击后，其影响完全可以和大规模杀伤性武器的破坏效果相提并论。

图 1：网络战作战样式



资料来源：互联网、东兴证券研究所

图 2：“震网”传播原理图



资料来源：互联网、东兴证券研究所

习近平总书记在网络安全和信息化工作座谈会上指出“网络安全的本质在对抗，对抗的本质在攻防两端能力较量。”因此，对于网空威胁行为体，特别是以美国情报机构为代表的超级网空威胁行为体的认知就构成了建立自身防御能力和威慑能力的重要前提。网络空间的博弈对抗也要建立客观充分的敌情想定，深入分析敌我当前的体系、能力、态势、装备、编制、战法等相关因素。要在未来的博弈竞合中占据主动，既要发挥我们的传统优势和积累，又不能拘泥于原有的视野和惯性；既要把美方作为一个超级网空威胁行为体来对待，又要把其作为一个能力引领方来看待。

网络安全攻防，防御成本急剧上升、碎片化安全问题严重。网络空间是一个以“工程”

方式构建的人造世界，由于现有 IT 系统复杂程度非常高，系统中总会出现无法及时发现的漏洞，加之国家支持型黑客集团往往水平高超、资源充足，且极富耐心，很难将其攻击行为长期阻挡在系统之外。尽早发现漏洞的捷径在于事先发现敌方的攻击行，为通过“漏洞分析和风险评估”的方式，透彻理解对手的行动方式，破敌“攻”而固己“防”。建一个更具弹性的安全系统，最大程度提升系统的抗攻击力，在自身系统与基础设施遭遇入侵的情况下仍可继续执行关键或基本任务。

根据网络安全研究机构SANS所提出的“滑动标尺”模型，将网空安全能力分五大类别，其中基础结构安全、纵深防御、积极防御、威胁情报等四大类别的能力都是一个完善的网络安全防御体系所必须的，而反制能力则是应当由国家级网空安全防御体系提供。在这些网络安全防御能力的支撑下，通过实战化的网络安全运行，实现全面完善的网空安全防御。

图 3：网络安全能力

资料来源：《网信军民融合》、东兴证券研究所

国际网络空间竞争博弈进入深水区。自 2015 年美国战略核心从“全面防御”调整为“攻击威慑”以来，各国在网络空间主导权、话语权争夺更加激烈。网络军事力量建设步入强体系、扩规模、提能力新阶段。

1.2 网络战四种战略作用

- **战略情报支援。**目前，人类社会绝大多数信息都以数据形式承载于网络空间，由此形成的数据信息域情报价值极高。**战略情报支援主要作用于数据信息域，通过多种网络入侵、口令破解、链路劫持等攻击技术手段，提取高价值信息。**与传统情报侦察手段相比，战略情报支援具有成本较低、风险较小、成果显著等优势，**平时能为国土防卫、外交斗争和政策制定提供决策依据；战时能为态势生成、目标识别和定点清除提供情报来源，已成为西方军事强国贯穿平战的首要获情手段。**美国在伊拉克战争中，由国家安全局运用网络入侵手段进入目标网络交换节点，经长期设伏监控，从中持续截获反政府组织重要人物的手机通话和电子邮件并分析其内容，为整体掌控安全态势、高效实施“猎杀”行动提供了准确及时的情报支援。

- **战略网系扰瘫。**网络运维域是网络空间的物质基础，由金融、能源、通信、传媒等关键业务网中的各类服务器、交换设备、传输设备等信息基础设施组成，一旦失调，

极有可能导致社会停滞、国家瘫痪。**战略网系扰瘫主要作用于网络运维域，以维系网络运行的主干链路和要害节点为目标，充分利用网络的广泛连通性及通信协议中的固有规则，通过发送“异态”报文或产生海量无用数据的方式，挤占计算资源和传输带宽，使目标因处于重复无效响应或严重过载状态而无法正常运转。**近年来，通过网系扰瘫阻滞对手社会经济体系关键环节运转的战略网络战手段发展迅速，部分军事强国已将其作为新型作战样式在联合作战中一体筹划，用于降低敌方民心士气和战争潜力，为己方顺利实施主要军事行动及实现国家战略目的扫清障碍、创造条件。俄格冲突中，格鲁吉亚政府、传媒、金融和军队系统 50 多家重要网站因大规模分布式拒接服务攻击而直接瘫痪，导致数个重要部门停摆，多支部队失控，甚至连外交工作都一度中断，整个国家陷入瘫痪和“失联”状态。俄军因此占据绝对信息优势，迅速调用兵力夺控关键地域，顺利达成预期目标。

- **战略实体操纵。**网络空间中的设备管控域，主要由大型制造、电力、交通等现代社会命脉行业中的网络化工业控制系统组成，事关行业稳定和国家利益，其战略价值得到多数国家的高度重视。近期多场局部武装冲突和地区政治危机中，都出现了战略实体操纵的“痕迹”，网络空间跨域攻击手段逐渐成形。**攻击方通过入侵工业控制系统强行改变部分重要设备正常工作状态，甚至施以超常规操作达成物理毁伤效果，直接扰乱或中断该行业的正常运转，进而引发社会动荡、国家发展受阻等严重次生效应。**克里米亚危机期间，乌克兰两家主要电力公司遭受实体操纵类攻击。攻击者取得电网主控系统部分控制权限后，强行断开多个断路器，导致数十座大型变电站“掉线”，引发较长时间大范围停电，超过 20 万民众生活受到影响，乌克兰政府的危机应对能力和公信力因此遭到严重质疑。

- **战略认知塑造。**信息时代，网络空间对各类社会活动呈现全渗透、全覆盖之势，已成为文化理念碰撞和意识形态对抗的主战场。网络受众域由使用网络的信息受众组成，是现代社会最庞大、最活跃且最易受鼓动的群体，其认知倾向和集体行为直接影响社会稳定和国家安全。**战略认知塑造充分利用了网络空间的社会“风向标”作用，瞄准网络受众域，通过信息植入、事件披露等手段对大批目标受众实施心理冲击或行为煽动，有意诱发群体性事件，甚至左右政局走向，引爆国家动乱，开启信息时代“不战而胜”的全新斗争模式。**2016 年美国总统选举期间，希拉里团队骨干成员约翰·博德斯塔遭受“钓鱼邮件”攻击，数千封敏感邮件被窃取并转交至维基解密网站。票选前夕，有关美国政府默许沙特和卡塔尔资助“伊斯兰国”，以及“克林顿基金会”接受巨额政治献金等事件遭到连续披露，直接影响了选情发展。

1.3 国际网络安全四大威胁

- **通过恶意使用通信技术，将信息和通信技术环境迅速转变为国家对抗的空间**

目前，利用信息技术实现军事和政治目标的领域已经大大增加。越来越多的专家投入到武器和军事装备系统应用人工智能的研究中，包括研究海、陆、空的信息基础设施等。据欧洲安全与合作组织的专家称，大约有 50 个国家正积极实施创造用于军事意图的恶意程序，并且，很多国家也有类似的计划。其中，有 10 个国家拥有庞大的军

事预算。很多媒体也报道了关于美国政府投入大量预算，研究恶意程序，并使用恶意程序对相关国家施压的内容。在信息技术环境中，实施强制行动手段的发展，也许会增加造成国际和平与安全冲突的风险。

- **利用全球媒体环境，特别是社会网络，使用强制手段解决国与国之间的争端**
- **由于信息和通信技术环境的无国界特性，使其在用于国际法的过程中，遇到困难**

网络空间的不确定性导致所有主权平等原则受到阻碍，也导致无法客观监控各国所应该履行的国际义务。使用计算机通信设备和网络进行的信息传输、转发与存储的虚拟性，使国际法的利益相关主体无法监测 ICT 环境中的风险，也无法在受害国中完全通过国际执法搜集有关证据。所以，ICT 环境的虚拟性所带来的风险，正成为履行联合国宪章关于和平解决争端第二条第三款的障碍。

- **网络恐怖主义与计算机犯罪相结合，并开始严重威胁关键信息基础设施的安全**

ICT 长期以来已然成为发达国家和发展中国家的威胁。对国际社会而言，反对将 ICT 技术用于犯罪目的的议题正变得日益严峻。第 27 届联合国预防犯罪和刑事司法委员会会议，于今年 5 月在维也纳召开。有史以来，会议第一次将打击网络犯罪定为主题。

网络安全已经不仅仅只涉及到企业内网和外网边界的安全问题，它已经从传统的网络安全本身，牵涉到了数据安全、业务安全、社会维稳和国家安全。

2. 各国网络攻防战略对比

2.1 美国

2.1.1 美国网络空间司令部

美国于 2017 年 8 月将网络司令部升格为一级作战司令部，2018 年 4 月，宣布将美军网络司令部升级为美军第十个联合作战司令部，地位与美国中央司令部等主要作战司令部持平，意味着网络空间正式与海洋、陆地、天空和太空并列成为美军的第五战场。“2019 财年国防授权法案”明确了网络威慑的路径和战略对手，给予美国防部发起军事网络行动授权。

表 1：美国网络空间国防发展轨迹

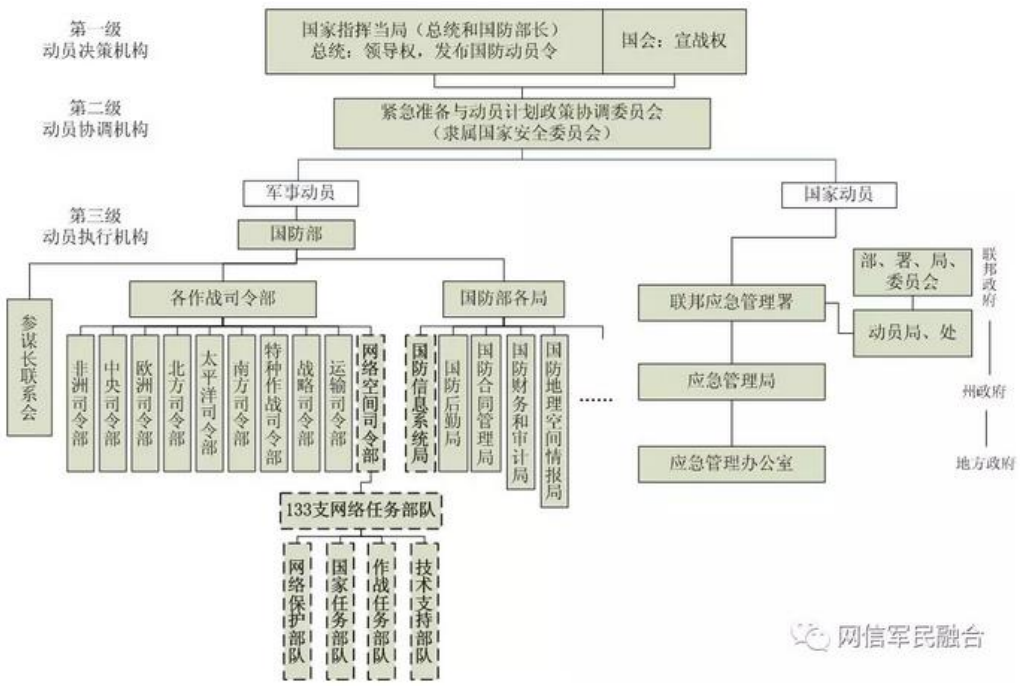
时间	事件	影响
2017.8	网络战司令部升级	升级后将成为美军第十个联合作战司令部，地位与美国中央司令部等主要作战司令部持平。网络战成为顶级战略作战方式
2016	举行“网络卫士”演习	提高在联合作战中实际运用网络战的能力
2015	国防部发布最新网络安全战略	提供网络安全综合能力，支持军事行动和紧急计划；建设并维护网络安全力量，为网络行动做好准备
2014	发布《四年防务审查报告》	将网络战列为 7 种作战能力之首，位于导弹防御、核威慑等能力之前；提出到 2019 年前，建设 108 个不同军种网络防护部队。
2011	发布《网络空间国际战略》	引发国际间网络军备竞赛

2009	组建网络战司令部	计划招聘 4000 名黑客，组建特种部队，统一协调保障美军网络安全和开展网络战等军事行动。
2008	《国家网络安全综合计划（CNCI）》	美国首次提出网域安全国家战略，信息安全战略地位提升。
2007	棱镜计划	对即时通信和既存资料进行深度的监听
2004 至今	爱因斯坦计划 2	部署基于签名的传感器，检测出试图非法进入联邦网络系统的互联网流量和恶意内容，形成入侵检测系统（IDS）
2004 至今	爱因斯坦计划 3	识别和描述恶意网络流量，增强网络安全分析、态势感知和安全相应能力，形成入侵防御系统（IPS）

资料来源：互联网，东兴证券研究所

美国网络空间国防预算近千亿人民币，未来国内有望诞生千亿产业。据 2016 年新华网的报道，美军从 2013 年年初开始组建网络部队，迄今已建成 123 支，总人数为 4990；未来的目标是在 2018 年建成 133 支具有全面作战能力的网络部队，总人数达 6187 人。美国网军包括网络作战部队、网络保护部队、国家任务部队三大机构。2016 年美国用于国防的网络安全预算已达 140 亿美元左右，2016 年初我国成立战略支援部队，下设网络战部队，如果对照美国的投入，则网络空间国防有望催生千亿产业。

图 4：美国国防及网信领域动员组织体系



资料来源：《网信军民融合》、东兴证券研究所

表 2：各国网络战抓总机构成立时间表

成立时间	国家	机构
2009 年	美国	网络战司令部
2014 年	俄罗斯	网络战司令部
2014 年	日本	网络安全战略本部

表 3：各国网络作战部队组建时间表

成立时间	国家	部队
2005 年	印度	网络部队
2013 年	日本	网络空间防卫队
2013 年	新加坡	网络防卫行动中心

2017 年	德国	网络信息空间指挥部	2017 年	俄罗斯	信息作战部队
2017 年	新加坡	国防网络署	2018 年	美国	133 支网络作战部队

资料来源：《网信军民融合》、东兴证券研究所

资料来源：《网信军民融合》、东兴证券研究所

美国网络司令部高调宣示指挥战略愿景文件，标志着网络空间对抗进入了新时代：2018 年 3 月，美国网络司令部在互联网公开其指挥战略愿景文件《获取并维持网络空间优势》，渲染网络空间安全威胁，针对性提出网络行动的目标、原则、任务和方法等，为各军种网络战部队统一思想和统一行动奠定基础。

■ **国家级攻防对抗将成为新常态，我国网络安全面临高压态势**

文件实质是为美国网络空间进攻型防御战略提供依据和指导方法，将网络空间战场边界直接推进到对手网络中，主动制造摩擦，增加己方行动自由，限制对手行动自由，通过攻击为主的手段塑造和影响对手，使对手只有招架之功而无还手之力，考虑到该文件中明确提到了中国威胁，预计未来我国网络空间安全将面临巨大压力。

■ **新形势下传统防护体系难以有效应对，网络防御重在构建敏捷性**

网络空间是一个类似流体的复杂开放空间，常态化接触对抗并且环境多变，不存在永久有效的防御或攻击手段，设计良好的防御体系往往存在风险。未来有效的防御思路是摒弃传统仅预设阵地、设卡布哨的做法，借鉴海空战中以灵活性应对不确定性的作战思维，以获取网络控制权为主要目标。打通网络中观测—决策—行动链条，把目前静态的安全能力动起来，使之具备灵活性，实现高度集成、按需加载和机动编组，以应对网络空间中的不确定攻击。

■ **为了实现敏捷灵活的网络防御体系，关键环节是发现已知/未知攻击**

国家级网络空间对抗级别更高、强度更大、范围更广，根据美国已泄漏网络战武器分析，除了组合加载、战术化利用已知攻击威胁外，还会更多地利用未知漏洞、未知攻击开展渗透破坏行动。传统依赖于事后分析提供的特征库或威胁库开展检测，难以全面、及时发现未知攻击，尤其是无法发现网络中长期潜伏，夹带在海量正常流量中的高强度、多类型远程渗透。

2.1.2 美军“网络航母”

2015 年，美国国防部在《网络空间战略》中首次推出“统一平台”（UnifiedPlatform，简称 UP）概念，目前已经进入实质性推动阶段，是其“军事网络作战平台”（MCOP）的重要组成部分。“统一平台”是一种可以携带网络攻击和网络防御武器，在网络空间自由穿梭的标准化平台，是美军为网络空间作战部队打造的主战装备，是美网络司令部迄今为止规模最大、最重要的采购项目之一，被形象称作“网络航母”（CyberCarrier）。

打造“网络航母”，整合各个分散的网络作战系统。截至目前美军已初步组建形成了 133 支网络任务分队，来自四大军种，人员总规模将近 6200 人，通过连续组织跨国、跨部门的“网络风暴”、“网旗”、“网络卫士”系列演习，各任务分队的网络攻防能力得到持续提升，美网络司令部各部门间的网络防御协作水平也逐年攀升。美军打造“网络

航母”这一标准化、规范化的作战平台，其关键意图就是整合各个分散的网络作战系统，打造标准化、体系化、通用化的军事网络作战平台，统一网络作战资源，统一指挥控制，提升其网络作战能力。

“网络航母”可携带搭载美军现有上千种病毒、木马及其他各类具有攻击性的网络软件，根据作战对手目标网络操作系统环境及网络架构特点，合理选择网络攻击资源，灵活选择适当的攻击方式，对于世界各个网络主权国家形成严重威胁。“网络航母”一旦建成并投入使用，美在网络空间的霸主地位将得到进一步巩固。

表 4：美军网络航母作战能力对比

对比项目	航母（AircraftCarrier）	网络航母（CyberCarrier）
作战空间	海上、水下、空中	网电空间（有线和无线）
作战系统	战斗机、攻击机、预警机、电子战飞机等各种舰载机以及导弹、火炮等自卫武器	病毒、木马、网络软件等
作战手段	火力摧毁目标	接入、控制、混乱、破坏目标
作战效果	夺取制空权、制海权	夺取制信息权
作战人员	需要精通装备性能、熟练掌握装备操作	只需经简要培训、按程序操作即可
截获概率	被敌发现概率高、隐蔽作战企图难	被敌截获概率低，隐蔽防护措施严密

资料来源：公开资料，东兴证券研究所

战术上突出针对性、隐蔽性、灵活性。“网络航母”项目“将整合现有的各军种能力，提供一种最小化可行产品（MVP），后续的迭代也将始终致力于提供一种灵活的、具有互操作性的和可扩展的作战能力，拥有自复制、自组网、自感知、自保护、自消亡等自我决策能力，为作战提供灵活的部署和攻击方式。

部署上突出持续、快速、高效。长期以来，美军奉行“全球部署、全球到达、全球摧毁”，目前美在海外部署有 374 个军事基地，分布在 140 多个国家和地区，在本土部署有 871 个军事基地，基本形成了“前沿少量存在，本土重兵机动”的战略布局，同时，美军还依托其海外空军、海军基地，牢牢掌控着巽他海峡、朝鲜海峡、马六甲海峡等海上咽喉要道，实现了美军在全球的军事存在，不断巩固和捍卫其在全球的各种利益。而“网络航母”一旦建成，美军网络作战司令部将会利用该平台，持续为实施网络空间作战任务规划、数据分析和首长决策提供强力支撑，“将现存的或即将出现的所有网络工具统一到一起”，最大程度满足各个网络作战部队的任务需求。

2.1.3 美国网络空间攻击与主动防御能力

美国具有国家安全至上的传统，从网络情报作业到军事行动，从网络空间攻击方式到网络主动防御计划，美国在网络空间具备自身的能力优势与特点。

从上世纪 40 年代开始，美国陆续通过“三叶草”、“尖塔”等计划，建立了对电报电话系统的监听存档机制，并从上世纪 60 年代开始建设以“梯队”为代表的各类信号情报获取系统，以形成情报网络基础。通过大型海底光缆监听、重点特殊区域监听、计算机网络利用（CNE）、运营商入侵、卫星监听、第三方情报共享等方式，美方能够在全球范围获取包括电子邮件、文件传输、语音通话、网络访问、短信、传真、电报等在内的各类网空信号情报，形成了网空作业的“先天优势”。特别是对于海底光缆

和运营商的窃听，使美方在信号获取和投入侧都具备了无与伦比的隐蔽性掩护和反溯源性优势。

在网空积极防御方面，美方建设了以 NSA 的“守护”为代表的积极防御体系。通过国家级的信号情报能力，提前获知对手的攻击意图、技术、工具等信息，将相应规则部署到边界的高速深包处理设备，在对手发动进攻时及时发现，快速响应。美方在网空防御方面十分重视利用民间技术和产品，高度尊重网络安全产品和服务价值规律，以 NSA 为例，商用网络安全产品是构成其防御体系的重要一环。在这些商用产品基础上，其形成了对威胁实现理解和环节整体防御框架体系，并进一步与国家战略情报相互协同。

图 5：美方网空作业技术流程与部分工程和装备作用的映射

资料来源：《网信军民融合》、东兴证券研究所

2.1.4 网络空间攻击支撑体系，重点推进持久化网空攻击装备

美国开展了一系列的网络空间进攻性能力支撑体系建设项目。其中最大的支撑架构称为“湍流”（TURBULENCE），由多个系统组成，包括主动情报采集系统 TUMULT、被动情报采集系统 TURMOIL、任务逻辑控制系统 TURBINE、进攻性网空行动系统“量子”（QUANTUM）、主动防御系统 TUTELAGE、密码服务 LONGHAUL、数据仓库 PRESSUREWAVE、网络流量分析系统 TRAFFICTHIEF 和信号情报分析系统 CLUSTER WEALTH-2 等。

- 被动情报采集系统（TURMOIL）：全球高速被动信号情报收集系统，用于拦截全球范围内传播的目标卫星、微波和有线通信。具备可以仿冒任何国家 IP 地址的高级反溯源能力。
- 任务逻辑控制系统 TURBINE：当 TURMOIL 的处理分析识别出重点目标时，TURBINE 进行进一步判定，是否需要对某个目标进行攻击。若判断需要，则会触发 TURBINE 系统程序，试图使用 QUANTUM 侵入目标计算机窃取信息。
- 进攻性网空行动系统 QUANTUM（量子）：能够向互联网侧目标部署作业工具，或

操纵已部署工具。通过多种方式劫持目标，包括应用广泛的“量子插入”（QUANTUMINSERT，针对 HTML 访问）和“量子之手”（QUANTUMHAND，针对 FACEBOOK 访问）等。

- 集成“关键得分”（X-KEYSCORE）项目：TURMOIL 会筛选出“有意义”的数据包，转发给 X-KEYSCORE，X-KEYSCORE 将会话数据化并通过 XKS 界面提供分析和搜索的功能，从而实现对网络空间攻击目标的发现与确定。

在这套支撑体系的支持下，美国的网络攻击行动能够获得强大的后端支持，各个系统各司其职，共同支撑信息收集、情报分析、积极防御、决策控制、网络作业等网空行动的攻击性行动环节，共同构成了美国强大的网络空间进攻性能力支撑体系。

美国秉承“持久化一切可以持久化的节点”的理念，将其作为重要战略资源储备，为长期的信息窃取和日后可能的网络战做准备。这既是进行网络情报获取等攻击性网空行动的基础，也是开展积极防御反制威慑、实现网络战攻击的重要前提。

在网络空间中，攻击方可在网络战开始前进行“战场预制”，通过对内网的穿透能力和对生产、运营商、物流链等相关环节的渗透，在网络战争开始前按照于己方有利的方式，攻击控制具有潜在战略或战术意义的网络设备和节点系统，从而隐蔽地实现对网络空间战场阵地的预制改造。战争开始后，就可以迅速将攻击载荷投递至已被持久化控制的关键位置，或者通过被持久化控制的阵地节点间接对关键位置发起攻击并投递载荷，从而通过攻击行动实现军事作战所需的网空攻击效用。

美国国家安全局（NSA）和美国中央情报局（CIA）均开发了大量具有持久化能力的网络攻击装备。NSA 的相关装备主要由特定入侵行动办公室（TAO）下属的先进网络技术组（ANT）开发。比较有代表性的装备包括针对 Juniper 不同系列防火墙的工具集 SOUFFLETROUGH 和 FEEDTROUGH、针对思科 Cisco 系列防火墙的 JETPLOW、针对华为路由器的 HEADWATER、针对 Dell 服务器的 DEITYBOUNCE、针对桌面和笔记本电脑的 IRATEMONK 等。

表 5：NSA 开发的具有持久化能力的网络攻击装备

名称	工作原理
SOUFFLETROUGH	是一种通过植入 BIOS 实现持久化能力的恶意软件，针对 Juniper SSG 500 和 SSG 300（320M/350M/520/550/520M/550M）系列防火墙。
JETPLOW	针对思科 500 系列 PIX 防火墙，以及大多数 ASA 防火墙（5505/5510/5520/5540/5550）的恶意软件，功能与 SOUFFLETROUGH 基本相同。
HEADWATER	是一个驻留型后门工具集，能够通过远程运营中心（ROC）远程传输到目标路由器。
DEITYBOUNCE	利用主板的 BIOS 和系统管理模块驻留在戴尔 PowerEdge 服务器中，操作系统加载时能够周期性的执行。
IRATEMONK	通过注入硬盘驱动器固件，针对桌面和笔记本电脑提供持久化能力。

资料来源：《网信军民融合》，东兴证券研究所

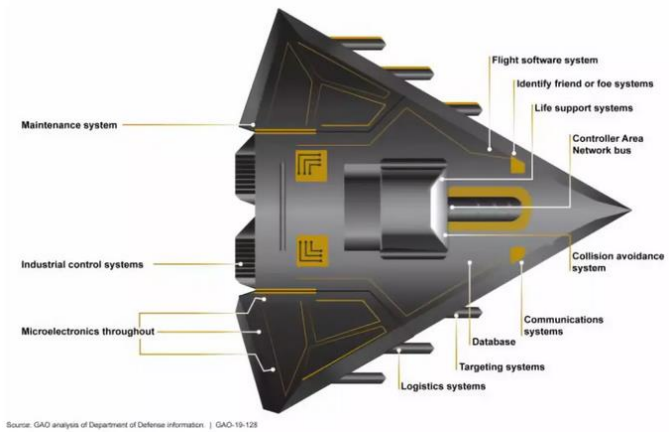
CIA 开发的持久化网络攻击装备，包括“暗物质”（DarkMatter）、“午夜之后”（AfterMidnight）和“天使之火”（AngelFire）等。DarkMatter 针对苹果主机和手机，

能够伪装成雷雳接口转换设备或进行固件植入，通过人力作业或物流链劫持实现攻击。AfterMidnight 是一个恶意代码植入框架，能够向目标远程投放恶意软件，伪装成 Windows 系统的.dll 文件。AngelFire 是一个针对 Windows 计算机的恶意代码植入框架，能够通过修改引导扇区的方式，在 Windows 系统中安装持久化的后门。

2.1.5 另一方面，美国防部（DOD）武器系统也存在网络安全漏洞

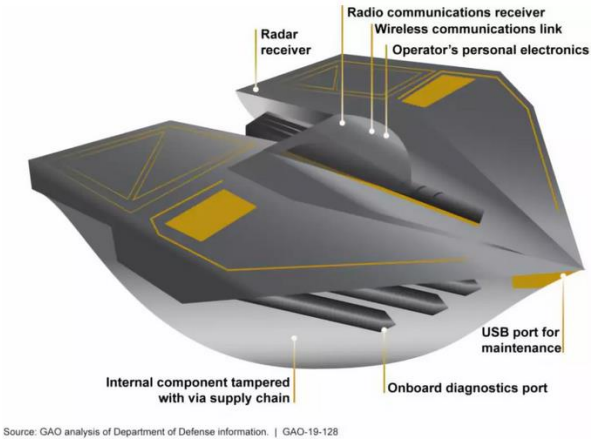
DOD 武器系统越来越复杂和网络化，网络漏洞也不断增加。DOD 武器系统越来越依赖软件和 IT 来达到预想的性能。目前武器系统中的软件数量正指数及增长，并嵌入在无数技术非常复杂的子系统中，这包括硬件和许多种类的 IT 组件。从最基本的生命支持功能到拦截发射的导弹，几乎所有武器系统的功能都是由计算机控制的。越来越依赖软件和 IT 明显增加了武器系统的攻击面（从网络安全角度被攻击的可能性）。

图 6：武器系统中嵌入的软件和 IT 系统



资料来源：、东兴证券研究所

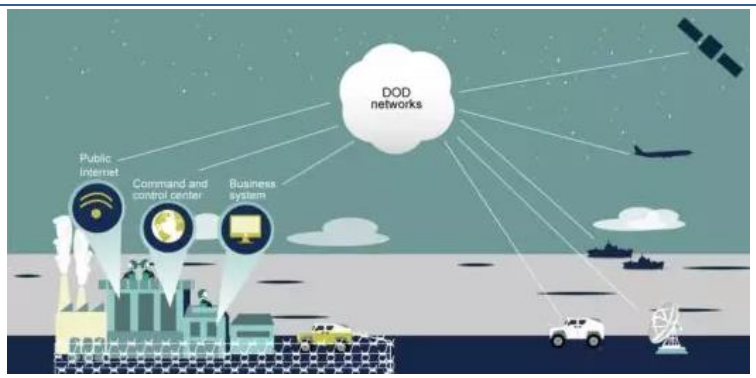
图 7：武器系统含许多可以被攻击者用于访问系统的接口



资料来源：、东兴证券研究所

DOD 武器系统比以前更加互联了，会引入漏洞并且使系统更加难以防御。武器系统连接到 DOD 的网络扩展集（DOD 信息网络）、甚至国防供应商这样的外部网络中。计算机系统、人力和其他商业相关的系统有时也会连接到武器系统连接的网络中。有些武器系统可能是不直接联网的，但是连接了电力系统这样的系统，而这类系统可能是直接连接到公网的。如果成功入侵了这类武器系统依赖的外部系统，就可能对武器系统的功能和有效性带来影响，甚至造成物理破坏和危害他人安全。

图 8：武器系统连接的网络可能连接了其他更多的网络



资料来源：《网信军民融合》、东兴证券研究所

目前，DOD 仍在寻求解决武器系统的网络安全问题，虽然武器系统与传统 IT 系统有许多相似处，但在武器系统中应用与传统 IT 系统安全系统的措施可能是不合适的。

2.1.6 俄罗斯网络安全战略

俄对信息安全高度重视，新时期保障信息安全战略目标和行动方向明确。受美苏两极冷战等历史因素影响，在实现信息化方面，包括信息基础设施建设进程、信息产业发展起步、信息技术发展水平等，俄罗斯都明显落后于西方发达国家。但也因此，俄对信息安全高度重视。早在 2000 年，俄联邦政府就出台了首份国家信息安全战略文件——《俄联邦信息安全学说》，正式将信息安全作为战略问题进行考虑，并就信息安全建设作出顶层设计和战略部署。随着信息安全威胁日趋复杂严峻，以及信息领域的国家利益不断扩大，俄联邦政府于 2016 年发布了首次修订版《俄联邦信息安全学说》，明确新时期保障信息安全的战略目标和行动方向。从俄信息安全战略的发展看，近年来俄对信息空间和信息安全的认识日益深刻，对信息安全建设的考虑更加全面和务实。

组建信息战部队，是俄军落实国家信息安全战略、维护国防领域信息安全的重要举措。新版信息安全学说明确，俄将提升联邦武装力量的信息对抗能力，包括完善信息对抗力量、改进信息对抗手段，以及提升信息威胁预警、发现和评估能力等，用以保障国防领域的信息安全。2017 年 2 月，俄军正式组建信息战部队，规模约 1000 人，主要职能是统一进行信息作战行动和管理，保护俄军事网络和站点，防止俄军事管理系统和通信系统遭到黑客攻击。

构建机制保障国家和社会领域信息安全。一是建立信息系统安全评估指标。俄信息安全部门制定了《计算机系统安全评估标准》、《产品安全评估软件》、《特殊环境下计算机系统安全评估标准使用指南》、《安全网络计算机系统安全评估标准说明》、《安全数据库》等一系列比较完善的信息系统安全评估指标。**二是建立信息安全认证及分级机制。**俄对信息安全企业和产品实行许可认证制度，并建有专门的认证机构和认证测试实验室。俄将信息安全等级划分为 A、B、C、D、E 五个等级，只有获得认证的信息安全产品，才能在市场上销售和使用。对于网络上的密码产品，认证条件则更为严格，密码保护设备必须是国内研制，并经相关部门鉴定。**三是建立网络检查和审核机制。**俄建立了较严格的互联网检查机制，允许监查经由互联网传播的信息，同时规定政府机构、事业单位及商业公司应将信息安全审核作为经常审核的安全项目之一。

加强信安人才培养为战略实施提供支持。一是构建信息安全人才培养体系。俄联邦政府将全国 90 所开设有信息安全专业的大学、22 个信息安全地区教学中心、12 个部委信息安全管理机构和科研机构组成一个信息安全人才培养体系登。**二是组建科学连培养信息战人才。**俄国防部自 2013 年起陆续在各军兵种院校和科研机构组建了 12 支科学连，用以吸引地方高校具有高科技专长的优秀毕业生入伍参与国防科研工作，并为之后组建的信息战部队输送人才。2015 年开办 IT 技术武备学校，并在军事通信学院开设信息安全专业，进一步完善信息人才培养机制。

积极推进信息安全技术的自主可控发展。一是自主研发处理器及操作系统。2010 年底，时任俄总理的普京签署命令，要求开发一款基于 Linux 的国产操作系统，以减轻对微软 Windows 系统的依赖。2014 年 6 月，俄宣布未来政府机构和国营企业，将不再采购以 Intel 或 AMD 为处理器的计算机，转而采用以国产处理器为核心的计算机；采购的计算机必需安装俄自主开发的 Linux 操作系统。**二是创建独立的域名系统（DNS）。**2017 年 10 月，俄联邦安全会议要求政府创建独立的域名系统根服务器，以应对西方国家对俄日益增强的网络空间安全威胁。**三是建设封闭式军事云存储系统。**俄国防部将投资 3.9 亿卢布（约合 3900 万元人民币）建设用于保密的封闭式军事云存储系统。目前，俄军已启动系统建设工作，预计 2018 年底完成大部分项目，整个系统的建设工作拟于 2020 年前完成。系统建成后将在各军区投入使用，最大限度地保护军用数据免遭破坏。

2.1.7 欧洲国家

德国是欧洲信息技术最发达的国家，向来重视网络空间的安全与发展，尤其注重国家网络安全行动的顶层设计。为有效应对网络空间的严峻挑战，构建安全的网络环境，促进国家的经济繁荣和社会稳定，德国政府于 2011 年推出首份国家网络安全战略，明确网络安全战略的总体目标和保障措施，用以指导和加强国家网络安全建设，并于 2016 年发布新版网络安全战略，对国家网络安全建设作出部署。与美国网络安全战略强调攻防能力并重发展不同，德国网络安全战略侧重于自身网络安全防护能力的提升，同时注重通过有效的国际协调行动促进网络空间的安全。

为应对网络空间的安全挑战，英国政府于 2009 年出台了首个国家网络安全战略，用以指导和加强国家的网络安全建设。2016 年 11 月， 英国政府发布的《2016-2021 年国家网络安全战略》提出进攻性网络能力涉及“故意侵入对手的系统或网络，意图将其破坏、瓦解或摧毁”。它提出进攻性网络是“我们全方位能力的组成部分，以遏制、剥夺对手在网络空间和现实空间攻击我们的机会”。为此，英国将投资国家进攻性网络计划，为相关人才提供所需的工具、技能和情报技术，发展利用进攻性网络的能力，并将该进攻性网络能力部署为作战整体能力的一部分，以增强军事行动的整体效果。

2018 年 2 月，法国公布的《网络审核报告》提出决策者可以依据对网络攻击行为的评估采取回应措施。该《报告》依据网络攻击造成的影响、严重性以及对法国主权、公众的损害程度将它分成五个等级，即从较小的攻击事件到紧急且严重的攻击事件，决策者可以将紧急而严重的攻击事件视作《联合国宪章》规定的“武力攻击”，从而触

发国家自卫权。这一分类机制为决策针对具体网络攻击作出回应提供了多种选择，而最终的所选措施是一项“政治决策”。

2.2 我国网络攻防能力急需提升，国家战略政策加快推进

2.2.1 网络空间防御能力严重滞后

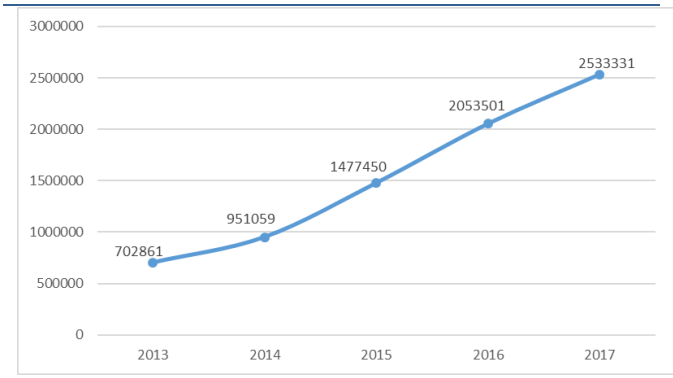
前期对网络安全的重视程度不够。我国是因特网高级持续性威胁攻击主要受害国，金融、能源、交通、教育等行业是“重灾区”。近年来电子政务、电子商务高速发展，但网络安全监管和防御能力严重“拖后腿”。网络安全投资占信息化建设总经费比例不足 1%，与美国 15%、欧洲 10%的水平差距甚大。既没摆脱高端技术受制于人现状，也没做到服务应用安全可控。网络攻击、信息窃取和破坏事件屡屡发生。

基础信息网络和重要信息系统隐患突出。有关部门对我政府机构、金融、电信、能源、铁路部门和军工企业等 120 多个单位 896 个信息系统检测，发现高危漏洞 1.2 万个。国家安全信息库显示，截止 2017 年 10 月，境内被植入后门的网站 2180 个，全国政务网站存在 3004 个告警信息，境内被篡改网站数量 5163 个，被木马或僵尸程序控制 IP 地址对应主机数 84 万个。仅 2018 年 12 月，境内感染网络病毒的终端数为近 78 万个；境内被篡改网站数量为 1,376 个，其中被篡改政府网站数量为 80 个；境内被植入后门的网站数量为 2,317 个，其中政府网站有 34 个；针对境内网站的仿冒页面数量为 5,324 个；国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞 1,206 个，其中，高危漏洞 481 个，可被利用来实施远程攻击的漏洞有 1,067 个。

■ **恶意程序**

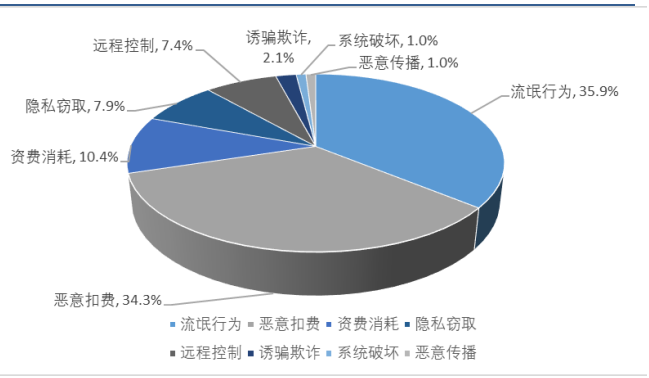
2017 年，CNCERT/CC 通过自主捕获和厂商交换获得的移动互联网恶意程序数量 253 万余个，同比增长 23.4%，增长比率近年来最低，但仍保持高速增长趋势。恶意行为，排名前三的分别为流氓行为类、恶意扣费类和资费消耗类[2]，占比分别为 35.9%、34.3%和 10.4%。

图 9：2013-2017 年互联网恶意程序捕获数量（个）



资料来源：国家互联网应急中心、东兴证券研究所

图 10：2017 年移动互联网恶意程序数量按行为属性统计



资料来源：国家互联网应急中心、东兴证券研究所

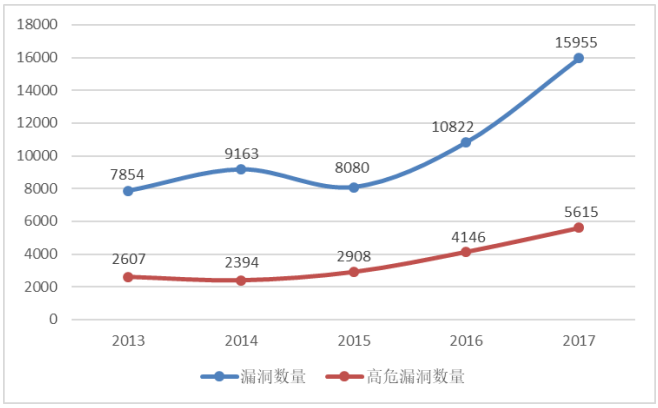
■ **安全漏洞**

近年来，国家信息安全漏洞共享平台（CNVD）所收录的安全漏洞数量持续走高。自 2013 年以来，CNVD 收录的安全漏洞数量年平均增长率为 21.6%，但 2017 年较 2016

年收录的安全漏洞数量增长 47.4%，达到 15955 个，数量达到历史新高。高危漏洞收录数量高达 5615 个（占 35.2%），同比增长 35.4%；“零日”漏洞 3854 个（占 24.2%），同比增长 75.0%。

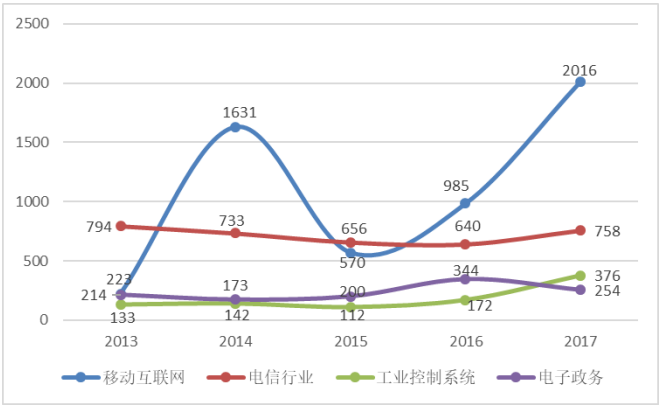
2017 年，CNVD 持续推进移动互联网、电信行业、工业控制系统和电子政务 4 类子漏洞库的建设工作，分别新增收录安全漏洞数量 2016 个（占全年收录数量的 12.6%）、758 个（占 4.8%）、376 个（占 2.4%）和 254 个（占 1.6%）。其中移动互联网、工业控制系统子漏洞库收录数量较 2016 年均有大幅上升，分别增长 104.7%和 118.6%。

图 11：2013-2017 年 CNVD 收录安全漏洞数量对比（个）



资料来源：国家互联网应急中心、东兴证券研究所

图 12：2013-2017 年 CNVD 子漏洞库收录情况对比（个）



资料来源：国家互联网应急中心、东兴证券研究所

■ DDoS 攻击

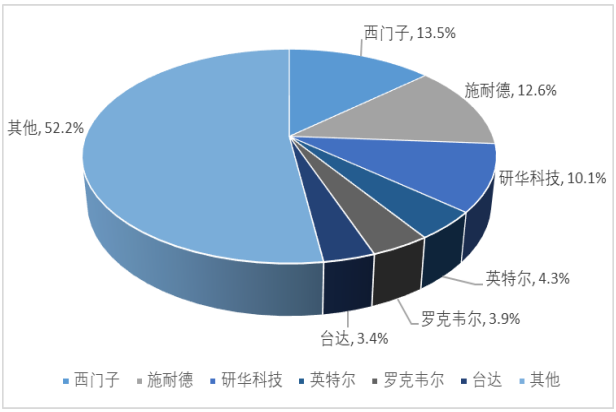
据 CNCERT/CC 抽样监测，2017 年我国遭受的 DDoS 攻击依然严重，攻击峰值流量持续攀升，且存在少量攻击资源被长期、反复利用发起大量攻击事件。

■ 工业互联网安全

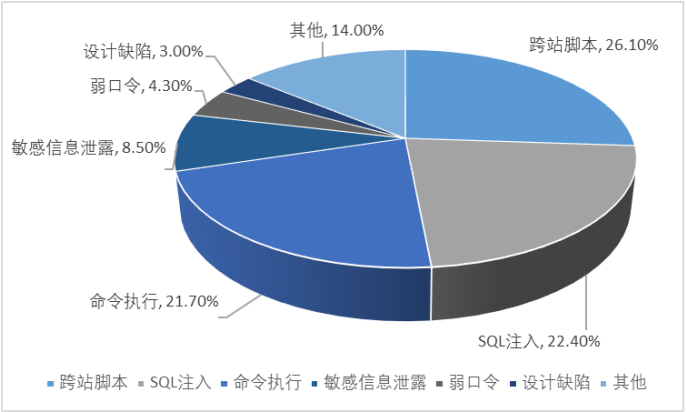
2017 年全年发现超过 245 万起（较 2016 年增长 178.4%）境外针对我国联网工业控制系统和设备的恶意嗅探事件，我国境内 4772 个联网工业控制系统或设备型号、参数等数据信息遭泄露，涉及西门子、摩莎、施耐德等多达 25 家国内外知名厂商的产品和应用。在 CNVD 工业控制系统子漏洞库中，新增的高危漏洞有 207 个，占该子漏洞库新增数量的 55.1%。

图 13：2017 年工业控制系统高危漏洞涉及厂商情况

图 14：2017 年互联网金融网站高危漏洞类型分布



资料来源：国家互联网应急中心、东兴证券研究所



资料来源：国家互联网应急中心、东兴证券研究所

■ **互联网金融安全**

2017 年，CNCERT/CC 抽取 1000 余家互联网金融网站进行安全评估检测，发现包括跨站脚本漏洞、SQL 注入漏洞等网站高危漏洞 400 余个，存在严重的用户隐私数据泄露风险，对互联网金融相关的移动 APP 抽样检测发现安全漏洞 1000 余个，严重威胁互联网金融的数据安全、传输安全等。

对进口信息设备几乎处在“不设防”状态。以芯片为例,不仅严重依赖进口，且不设置任何门槛，甚至允许外国公司直销，外企直接掌握每台机器信息。

安全技术落后。当前我国网络安全主要依赖防火墙、杀毒软件和入侵防御系统，没有形成全局性态势感知技术能力和应急响应机制，面对大规模网络攻击无还击之力，有人形容，“中国几乎赤身裸体地站在已经武装到牙齿的敌人面前”。

2.2.2 国家战略政策加码、军队信息化建设推动发展

网络安全重要性凸显，国家战略出台指导行业发展。2013 年以来，我国先后成立了国家安全委员会、中央网络安全和信息化领导小组，出台了《国家安全法》、《网络安全法》、《国家网络空间安全战略》、《网络空间国际合作战略》等法律法规和重要指导文件；习近平主席更是发表了“没有网络安全就没有国家安全”的重要论述，国内自上而下对网络安全的认识和重视空前提升，我国网络安全产业进入的发展新阶段。

等保 2.0 标志着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。

表 6：近年我国网络安全方面主要政策

2012 年 12 月 28 日	全国人大常委会通过《关于加强网络信息保护的决定》
2013 年 6 月 8 日	中美将在战略安全对话框架内设网络安全工作小组
2013 年 6 月 14 日	外交部设立网络事务办公室
2013 年 11 月 12 日	中央决定成立国家安全委员会
2014 年 2 月 27 日	中央网络安全和信息化领导小组成立

2015 年 7 月 1 日	《国家安全法》公布施行
2016 年 3 月 25 日	中国网络空间安全协会成立
2016 年 4 月 19 日	习近平在网络安全和信息化工作座谈会上发表 419 重要讲话
2016 年 8 月 22 日	中央网信领导小组发布《关于加强国家网络安全标准化工作的若干意见》
2016 年 10 月 17 日	工信部印发《工业控制系统信息安全防护指南》
2016 年 12 月 27 日	国家网信办发布《国家网络空间安全战略》
2017 年 3 月 1 日	外交部和国家网信办发布《网络空间国际合作战略》
2017 年 6 月 1 日	《网络安全法》正式实施
2017 年 6 月 9 日	网信办、公安部、工信部等四部委发布《网络关键设备和网络安全专用产品目录（第一批）》
2017 年 10 月	十九大报告提出，加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间；提高基于网络信息体系的联合作战能力等。
2018 年 4 月 20 日	全国网络安全和信息化工作会议，习近平就网络安全发表重要讲话。
2018 年 6 月 27 日	公安部发布《网络安全等级保护条例(征求意见稿)》（等保 2.0）

资料来源：互联网，东兴证券研究所

随着国家战略、制度法律的完善，网络安全的制度阻碍被逐步扫清。但**由于在战略部署、历史发展、网络安全意识上仍然落后于美国，还需进一步加码技术层面的提升，不断发展军事信息化，依托军民融合的方式提升我国网络攻防能力。**

成立战略支援部队，推动军队网安需求增长：2015 年 12 月 31 日，中国人民解放军成立第五大军种——战略支援部队成立。习近平强调战略支持部队是维护国家安全的新型作战力量，是我军新型作战能力的重要增长点。战略支援部队涉及情报、技侦、特种作战、电子对抗、网络攻防、心理战、后勤保障、装备保障等领域，是我国网络空间国防力量的主要组成部分。战略支援部队的组建有望拉动军队对于网络安全设备与服务的需求。

2019 年为军队信息化重大节点：《2006 年中国的国防》白皮书明确表示，国防和军队现代化建设到 2020 年，基本实现机械化，并且信息化建设取得重大进展；到 21 世纪中叶，基本实现建设信息化军队、打赢信息化战争的战略目标，基本实现军队国防现代化。我国军事编制改革持续推进，为实现机械化和信息化双重跨越做足准备。十九大报告提出，“扎实做好各战略方向军事斗争准备，统筹推进传统安全领域和新型安全领域军事斗争准备，发展新型作战力量和保障力量”。

3. 对标美国火眼公司，探索网络安全军民融合新思路

3.1 具备网络安全核心技术，并购建立综合安全管理平台

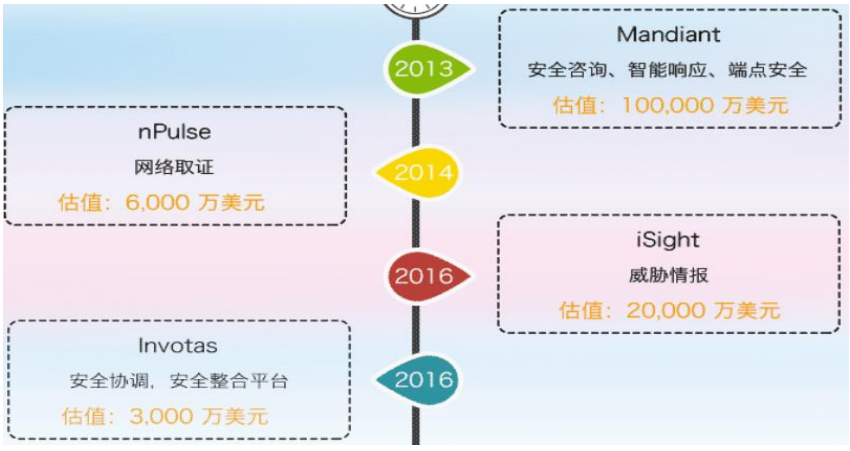
FireEye 于 2004 年成立，随着 0 day 漏洞利用和 APT 攻击的猖獗开始不断兴起。0 day 是未被发现的漏洞，即产品原开发商尚未修复、甚至未知的漏洞；APT（高级持续威胁）是一种以特殊利益（通常为商业和政治利益）为目的，针对类似政府、企业、军队等组织发动具有潜伏性、针对性的攻击。APT 是对组织网络的破坏，组织网络上任何一个节点的薄弱都会引起系统性的破坏。

FireEye 的核心在于 MVX 技术（Multi-Vector Virtual Execution），在 APT 防御领域独步武林。MVX 是一种“无特征码”的技术，采用 MVX 技术的产品会将邮件附件放到虚拟的“沙盒”中，然后观察附件在这个虚拟环境中的行为。能够在虚拟机上复制客户的网络环境，当恶意软件发起攻击时，虚拟机可加快时钟走时，在几微秒的时间内了解其连续数月的攻击行为；VX 引擎还可同时模拟多个系统环境（比如 Windows、Office 等），来同步判断是否存在威胁，产品效率相当高。沙箱技术虽然在 APT 防护领域已经广泛使用，但 MVX 仍然是最优秀的技术之一。

并购扩张规模，建立综合安全管理平台。2012 年 6 月，全球最大的安全技术公司迈克菲（McAfee）前总裁兼 CEO Dave De Walt 正式加盟公司，担任 FireEye 董事会主席；同年 11 月，Dave De Walt 被任命为 FireEye 的 CEO。Dave De Walt 是一名并购专家，自 Dave De Walt 入主以来，FireEye 发起了多宗并购事件，将 FireEye 的规模迅速扩张变大。这些并购对象主要从事网络安全咨询与舆情控制、威胁情报和安全整合业务，通过并购，FireEye 实现了在安全服务领域较大的跨越，搭建起了以侦测、响应、情报、咨询为一体的综合安全管理平台。

2013 年 9 月 20 日，FireEye 在纳斯达克敲钟上市，融资 3.035 亿美元。其后开展的并购案件主要有：2013 年 12 月 30 日，逾 10 亿美元收购网络安全公司 Mandiant；2014 年 5 月 8 日，6000 万美元收购大数据安全分析公司 nPulse Technologies；2016 年 1 月 20 日，2 亿美元收购领先威胁情报公司 iSIGHT Partners；2016 年 2 月 1 日，3000 万美元收购安全信息平台公司 Invotas。这四家公司主要从事网络安全咨询与舆情控制、威胁情报和安全整合业务。

图 15：火眼公司上市后的重要并购案件

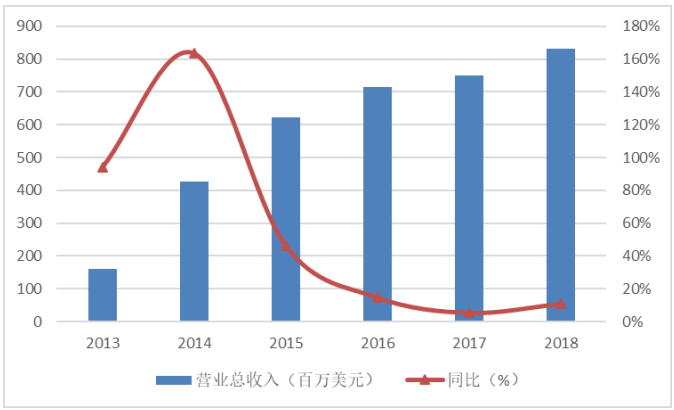


资料来源：公开网络、东兴证券研究所

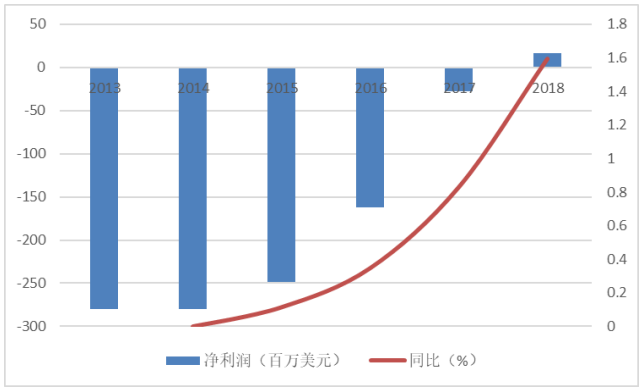
2011-2015 年，FireEye 的客户规模从 450 家直线增长到 4400 家，年复合增长率高达 76.83%。截至目前，FireEye 在 67 个国家拥有超过 5300 个客户，其中包括福布斯全球 2000 强中的 800 多个客户。不过 FireEye 的客户仍主要来自美国国内市场，比重从 2012 年的约 80%下降至 2015 年的约 70%。

图 16：火眼公司 2013-2018 年营业收入及增速

图 17：火眼公司 2013-2018 年净利润及增速



资料来源：Wind、东兴证券研究所



资料来源：Wind、东兴证券研究所

至今，FireEye 业务线可以分为三大领域，威胁防御、分析响应、安全服务：

威胁与防御，以网络安全 NX、邮件安全 EX、移动安全 MX、端点安全 HX、文件安全 FX 等安全设备为基础，构建在中央管理系统 CMS 下 APT 检测与防御网络。

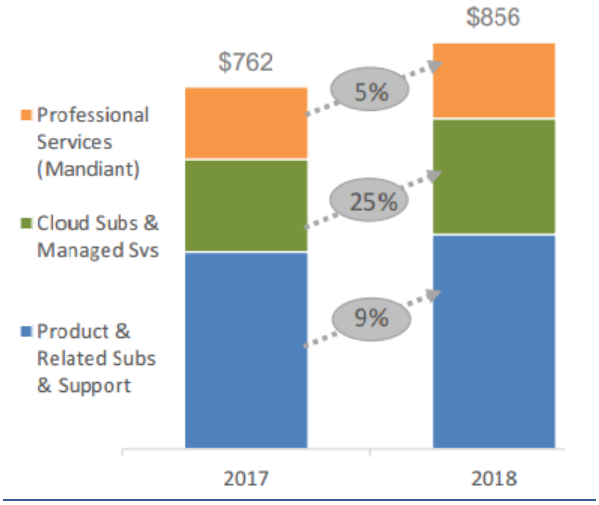
分析与响应，由恶意行为分析 MA、威胁分析平台 TAP、安全协调 SO 和安全取证 Forensics 等系统组成，结合威胁防御平台建立的威胁分析、取证平台。其中，FireEye 的取证系统取得了美国国家安全局的认证，可用于司法认定。

安全服务，包括了火眼即服务 FaaS、威胁情报等服务。其中，火眼即服务 FaaS 会有相应的专家会跟踪系统的异常事件，对发生的异常快速反应，并能够快速记录下攻击的证据，作为系统遭受依据。

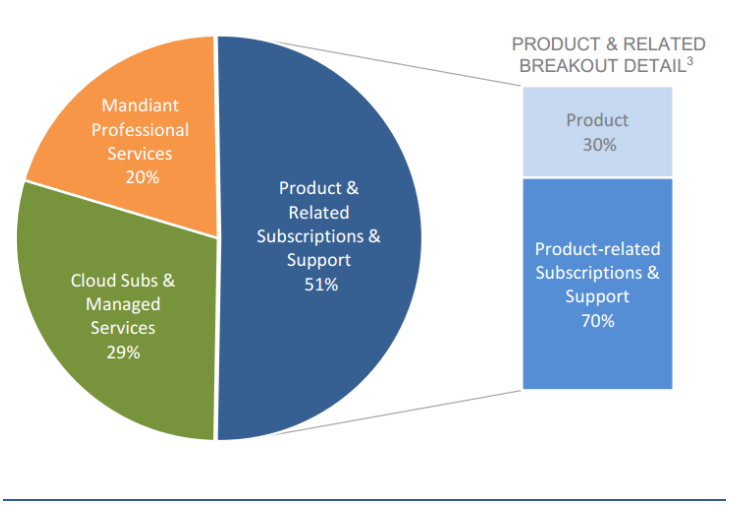
2018 年公司专业服务（Mandiant 咨询）、云计算服务的营业额分别增长 5%和 25%，两项服务类业务营业额之和占比接近 50%。随着公司在服务类业务上的增长，公司净利润摆脱负增长，进入正常增长阶段。**卫士通近年逐步布局的安全运维、安全飞天云等新业务，正处于起步阶段，对标火眼公司，预计未来将有较大增长空间，有望占据主营业务的半壁江山，或再造一个卫士通。**

图 18：火眼公司 2018 年各业务营业额增速

图 19：火眼公司 2018 年各业务营业额占比



资料来源：公司官网、东兴证券研究所



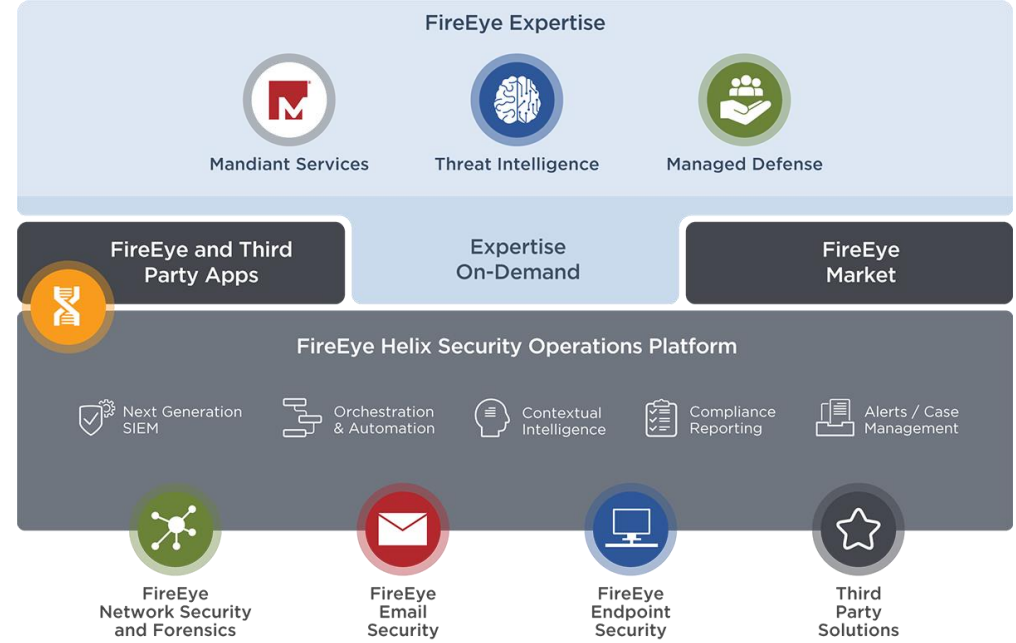
资料来源：公司官网、东兴证券研究所

3.2 FireEye“生态系统”

FireEye 生态系统结合了技术和专业知识，以实现最佳安全状态。在统一的安全运营平台 Helix 下提供一整套检测、保护、调查功能，包括网络，端点和电子邮件安全解决方案。而 Mandiant 咨询，托管防御和威胁情报服务可为组织提供必要的资源和知识，以响应和保护组织免受最高级威胁的侵害。

- 托管防御（Managed Defense）：应用攻击者的前端信息和经过验证的狩猎方法来检测和响应隐蔽活动。
- Mandiant 咨询：应对全球范围内的重大入侵，提供网络安全咨询服务，以防范网络威胁。
- 威胁情报服务（Treat Intelligence）：为安全团队提供前瞻性、高保真度、以对抗为中心的情报和可行建议。

图 20：FireEye“生态系统”



资料来源：FireEye 官网、东兴证券研究所

FireEye 威胁情报是基于设备平台的一部分，以订阅形式销售全球威胁情报，可帮助中小企业和大型企业了解全球威胁情况，并帮助客户识别网络和系统数据泄露事故的威胁行为者和指标；自动防御零日威胁和其他高级网络攻击。

提供 5 种不同的情报订阅，专门为不同的安全工作角色而设计：

- 战术情报：针对战术性技术性用户，该基本订阅服务提供丰富的数据源和警报。
- 操作情报：针对安全运营中心（SOC）人员以及事件响应（IR）团队，此订阅服务提供可操作内容，例如威胁行为者和恶意软件配置文件，以及数据源和情报。还包括优先级过滤器，以帮助安全人员首先关注高优先级威胁。
- 融合情报：该情报中的分析报告和技术情报可帮助 SOC 和 IR 人员搜索攻击者，根据企业网络风险配置文件而定制。涵盖“操作情报订阅”中所有内容，包括防御方案、行业分析等。
- 高管情报：该订阅服务针对首席信息安全官以及管理人员，为他们提供精简的非技术信息来做出风险、投资和战略决策。
- 漏洞情报：此订阅服务主要针对负责确保补丁管理执行以及评估和优先排序漏洞的 IT 人员。包括修补程序的信息，以及新兴威胁信息。

此外，还通过 FireEye 安全专家提供全天候监控、应用情报和威胁检测，FireEye 安全专家会与客户现有托管安全合作伙伴合作。客户会收到有关攻击者、攻击意图和响应指导意见的报告，作为订阅服务销售。

3.3 政企合作、军民融合在美国网络空间建设的典型案例

FireEye 作为安全界的神话之一，其在 2012 年后能够获得快速发展壮大，不仅恰逢当时全球网络安全环境需求新技术的大背景，以及新生领导力量的入驻，还包括美国军民融合模式对产业发展的巨大推动力。

1）美国中情局（CIA）的风险投资部门 In-Q-Tel 对于 FireEye 的早期发展给予了一定的帮助和引导，并保留了 FireEye 小部分的股份（少于 1%）。In-Q-Tel 是专为 CIA 提供风险投资服务的独立非营利机构，它的主要任务是对具有重要战略价值的尖端创新技术进行有针对性的投资，并借助这些最新技术强化美国在信息情报方面的搜集和监控能力。因此，美国情报部门是 FireEye 的重要客户之一，FireEye 的客户包括 40 多家情报机构。

2）FireEye 与美国国防部和军事部门有着密切的合作。2014 年，隶属于美国国防部的国家安全局（NSA）通过评估供应商对“国家安全系统”所有者和运营商的服务一致性，根据“国家安全网络援助计划”，向 7 家网络安全企业授予了“网络事件响应援助认证”，其中就包括 FireEye 以及被其收购的网络安全公司 Mandiant。其次，2015 年，时任美国国防部长阿什顿·卡特发布网络战争新战略时也表示，政府与 FireEye 等私营网络安全企业之间的更强劲伙伴关系大大提高了美国国防部的应对能力。此外，美国众多国防工业承包商、军工企业和航空航天部门等都是 FireEye 的客户。

3）FireEye 与美国多个联邦政府部门有合作关系，美国白宫、国务院等机构都是其重要客户。2013 年 FireEye 的产品就已经覆盖了 60 多个美国重要的联邦政府部门。2015 年，FireEye “MVX 引擎”和“DTI 云平台”获得美国国土安全部（DHS）SAFE TY Act 法案认证。FireEye 因此成为第一家得到国土安全部认证授予的安全企业。根据该认证，使用相关 MVX 和 DTI 产品的企业客户，可免于一些诉讼：他们的用户不能以公司技术无法抵御网络恐怖袭击为由进行起诉。DHS 的认可使得 FireEye 的市场继续得到扩张。此外，FireEye 还与美国联邦调查局密切合作，积极协助网络犯罪的调查和取证。

4）美国政府出于网络安全的考虑，以及网络安全核心技术领域对知识产权的保护，要求 FireEye 的产品对中国禁售。作为对 FireEye 放弃中国大陆市场的经济补偿，美国要求政府机构和大厂商（包括大的 IT 寡头和军工集团）部署 FireEye 的反 APT 产品，从而推动了 FireEye 在全美的集中商业部署和迅速发展壮大。

美国的军民融合、公私合作以及特有的“旋转门”机制成为以 FireEye 为代表的新锐厂商得以快速成长的基石和助燃剂，为美国网络安全领域创新技术的发展以及整个网络安全产业生态的形成和成熟提供了肥沃的土壤。政企合作、军民融合始终是美国网络空间力量建设与运用的基本思路，其在网络空间军民融合方面的做法与经验，对我国网络空间力量建设和网络安全产业发展具有重要的借鉴意义。

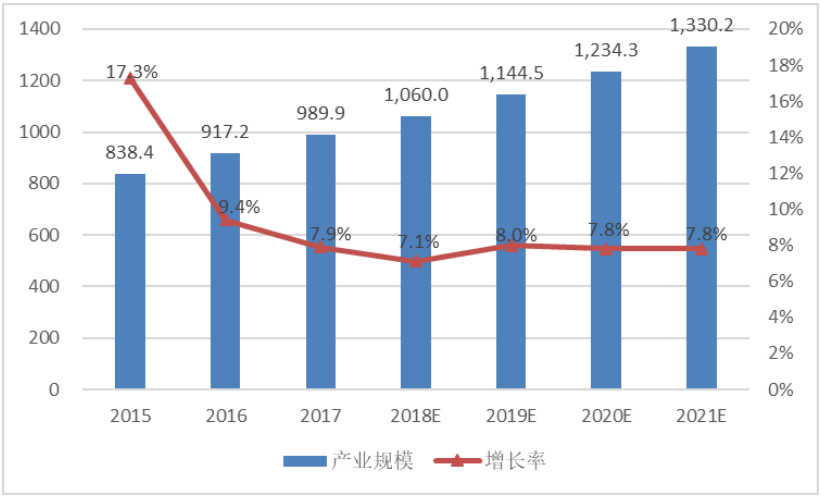
4. 网络安全产业发展出现新趋势

4.1 网络安全行业加速增长

全球安全产业规模稳步增长。2017 年全球网络安全产业规模达到 989.86 亿美元，较

2016 年增长 7.9%，预计 2018 年增长至 1060 亿美元。从增速上看，全球安全产业增速在 2015 年达到历史高位 17.3%，随后回落至 7.9%的增长水平。

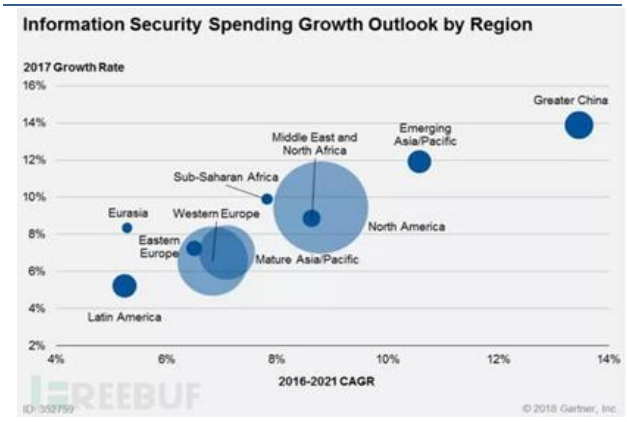
图 21：全球安全产业增长情况



资料来源：Gartner、东兴证券研究所

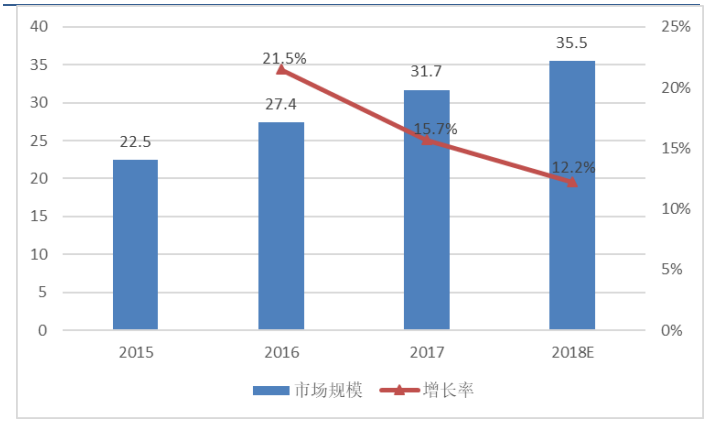
区域格局保持稳定，北美、西欧、亚太维持三足鼎立态势。在区域分布方面，北美、西欧、亚太维持三足鼎立态势，合计市场份额超过 90%。其中，美国、加拿大为主的北美地区 2017 年产业规模达到 408.76 亿美元，较 2016 年增长 9.2%，市场规模全球占比 41.29%，占据全球最大份额；英国、德国、芬兰等 16 个西欧国家 2017 产业规模合计 267.29 亿美元，同比增长 6.5%全球占比为 27%；日本、澳大利亚、中国、印度等 10 个亚洲国家 2017 年产业规模合计 225.08 亿美元，同比增长 9.5%，全球占比 22.7%。

图 22：2016-2021 全球各区域安全支出增长情况



资料来源：Gartner、东兴证券研究所

图 23：国内网络安全产业增长情况



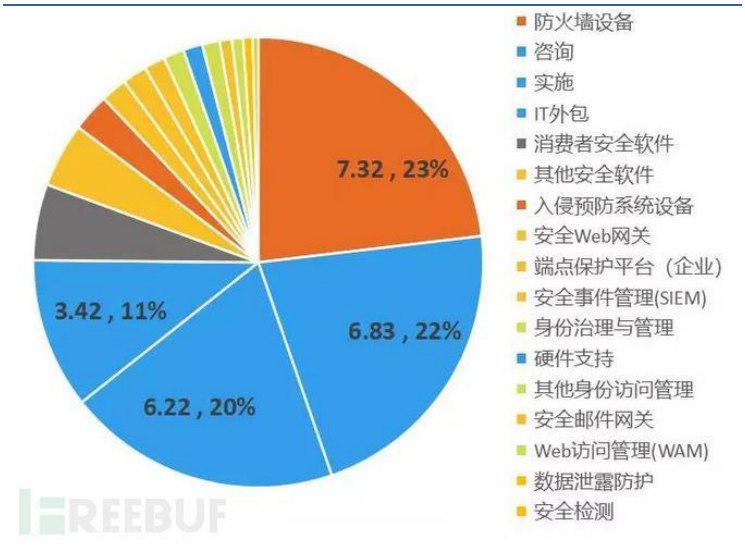
资料来源：Gartner、东兴证券研究所

根据 Gartner 数据，2017 年中国网络安全产业规模约为 31.7 亿美元，增速略微下降为 15.7%。其中，防火墙设备、咨询、实施和 IT 外包占据中国四分之三的市场。

全球安全服务与安全产品市场保持六、四分格局，防火墙、安全检测引领细分领域增长。细分市场中，防火墙、安全检测工具、身份识别与访问控制产品、安全外包服务

引领细分产业增长。其中，防火墙市场依然保持高位增长，2017 年市场增速达到 15.8%，主要是受益于数据中心等大规模网络的部署、大型企业集中化管理以及传统产品升级需求；安全检测工具 13.9%，基于内部风险的安全事件频发，进一步引发了网络安全隐患排查的需求，企业日益重视通过有效工具和手段以识别、评估内部风险和脆弱性；身份识别与访问控制产品，增速为 13.6%，驱动因素主要有两方面：一是移动化办公引发的终端和用户管理需求，二是云应用的快速增长。

图 24：2017 年中国安全细分市场规模情况



资料来源：Wind、东兴证券研究所

图 25：2017 年全球网络安全细分市场规模

资料来源：Wind、东兴证券研究所

4.2 网络安全行业技术发展趋势与新增需求

国内网络安全市场正悄然发生巨变。传统网络安全产品主要集中在防火墙、入侵检测和杀毒软件，称为“老三样”。“老三样”从 1995 年一直到现在，依然有很大的存量市场，再加上周边的硬件等产品，现在的总体规模在 500 亿到 600 亿左右。随着这几年移动互联网、云计算、工业互联网、物联网等技术的发展，以及对数据、业务安全的重视，网络安全开始往更广的范围发展。

图 26：网络安全领域扩展趋势图

资料来源：《网信军民融合》、东兴证券研究所

4.2.1 数据安全和应用安全成为行业新增长点

数据资产急速增长，传统边界安全转向内容安全和数据安全。随着云计算、大数据、物联网、移动互联网的兴起，企业用户的数据急剧增长，数据日益成为驱动企业发展的核心资产；与此同时，新的应用场景不断涌现，个人随身携带的数据资产呈指数级增长。

传统的网络安全产品偏向于边界防护，但互联网边界变得越来越模糊，在目前安全领域的快速变革发展下，数据安全和内容安全进入公众视野，安全厂商也开始深度布局、产品研发。

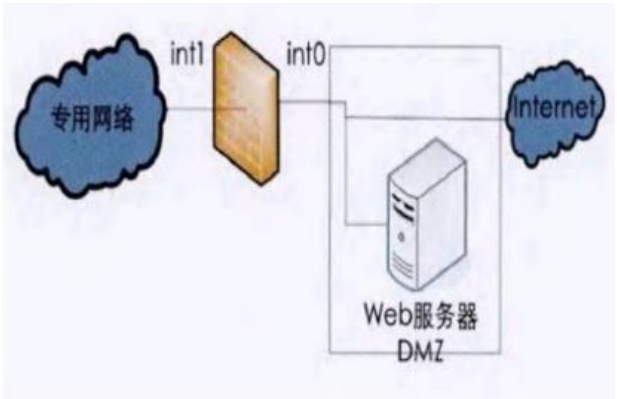
数据安全涉及众多环节，网安公司布局各有侧重。数据安全产业链包括数据交换安全、数据隔离、数据存储、数据加密、数据取证、数据监测等环节。目前国内的网安厂商中，卫士通在数据加密领域目前已经成为国内龙头，公司是国内唯一一家同时拥有普密、商密领域最高级别资质的信息安全企业，也是目前国内以密码为核心的信息安全设备的最大供应商，电子政务内网以及商密国产化项目将为传统加密业务带来新的机遇。启明星辰的数据安全业务主要通过其子公司合众数据进行，旗下产品包括数据交换、数据隔离、大数据应用服务平台、可视化平台等。

4.2.2 云安全带来虚拟化需求，成为云-网-端立体式安全核心

传统网络安全更偏向于“网”端安全，即网络系统的硬件、软件及其系统中的数据受到保护，不因偶然或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断，主要通过边界防护来实现。“云”端安全指的是面向云架构的，对平台及平台上资料的安全性、可用性和保密性的保护。而“端”的安全主要指终端，在当前的形势下更多是移动端从物理层到应用层的全方位防护。

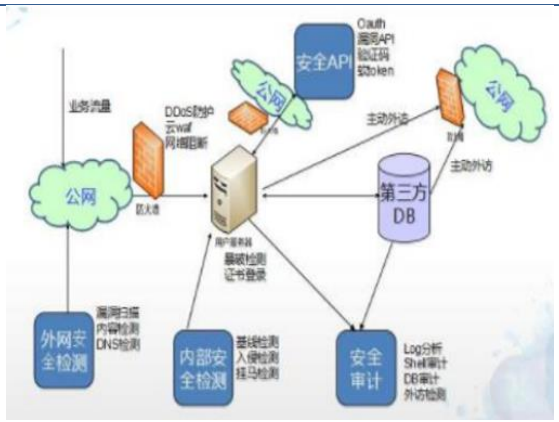
云安全包含传统安全需求，也包括虚拟化带来的安全需求。传统架构存在明显的网络边界，“互联网-防火墙-DMZ 区-主机区-终端”的层级十分清晰，网络安全检测和防御设施主要部署在防火墙和 DMZ 区上。然而云安全使用了虚拟化的技术，使得虚拟机可以比较简单的创建、删除、数据通信和数据迁移，保护范围从物理主机延伸到每一个虚拟机上。云架构系统面临的网络安全问题包含了传统的信息安全，如账号管理和身份识别问题、病毒和木马等恶意代码的攻击、拒绝服务攻击等。还包含由于虚拟化所带来的云架构特有的安全需求，如虚拟机可信级别不同所带来的问题、安全级别无法及时更新的问题、虚拟机蔓延的问题、虚拟机迁移和删除所带来的安全漏洞等。

图 27：传统系统安全架构



资料来源：互联网、东兴证券研究所

图 28：云架构系统安全体系



资料来源：互联网、东兴证券研究所

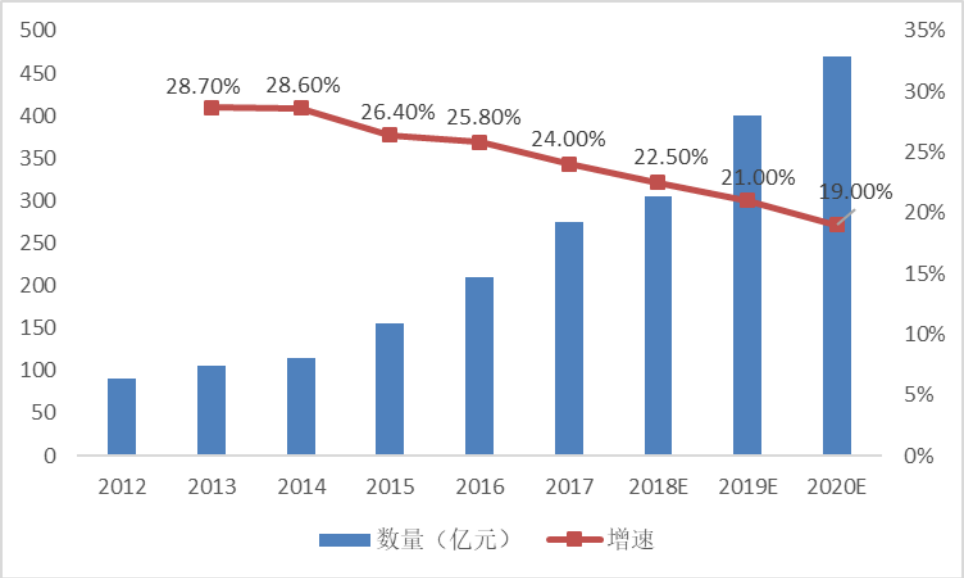
云安全可与多种技术相结合，发展前景广阔。云安全可与大数据、人工智能等技术相结合，利用大数据对安全模型进行训练。绿盟科技的“态势感知”产品就是这种结合的典型产品。云安全可在物联网中发挥更大的作用，所谓物联网，就是移动设备将数据上传到云端，再有云端实现对端设备的控制，从而实现“万物互联”。因此，如何将云安全，特别是端设备的云安全应用于物联网设备中是云安全的一个研究方向。

4.2.3 物联网安全和工控安全兴起

与物联网相关的攻击将发展出比海量 DDoS 攻击更危险的攻击形式。近年来，大量由僵尸网络驱动的 DDoS 攻击利用被感染的物联网，通过向受害者网站发起大量流量为攻击手段，最终造成严重后果。安全性较差的物联网设备也成为攻击目标，针对控制关键基础设施的物联网设备的攻击数量将不断增加，如配电与通信网络。

联网终端数量呈数量级增长，物联网安全市场规模将远超互联网。重点关注设备与功能安全，尤其注重传感端数据和控制端设备的安全。根据 CompTIA 的预测，到 2020 年联网的终端设备数将达到 501 亿台，但联网渗透率仍仅 3%。即使如此，由于物联网的感知设备遍布几乎所有物理度量参数的采集，数量远超过互联网中的智能终端数，并且物联网的感知节点计算机能力较弱容易被攻击，预计物联网带来的安全市场将远超过互联网。

图 29：联网的终端设备数量快速增长



资料来源：CompTIA、东兴证券研究所

工控安全事件频发，引起损失严重。工控安全指的是 ICS 的功能安全、信息安全等一系列防护策略和手段，主要是通过防攻击、防篡改、防病毒、防瘫痪、防窃密等方式来实现设备和工厂的正常运行，并保证工业信息和数据的机密性、完整性、可用性。近年来，工控安全事件频发，造成损失十分巨大。如 2010 年“震网”蠕虫病毒入侵伊朗布尔什尔核电站，导致 20%离心机报废，约 3 万多个网络终端被感染，伊朗发展核事业的进程受到重大打击。

工控安全标准已经建立，工控系统安全建设有望加快推进

表 7：近年中国关于保障工控安全的政策

时间	工控安全事件
2005.2.1	《电力二次系统安全防护规定》
2011.9.29	工信部 451 号文《关于加强工业控制系统信息安全管理的通知》
2012.6.28	国务院发布《关于大力推进信息化发展和切实保障信息安全的若干意见》
2013.3.13	《电力工控信息安全专项监管工作方案》
2014.3.24	《烟草工业企业生产网与管理网网络互联安全规范》
2015.5.19	《中国制造 2025》
2016.5.20	《国务院关于深化制造业与互联网融合发展的指导意见》
2016.10.17	工信部《工业控制系统信息安全防护指南》
2016.11.7	发布《网络安全法》-关键信息基础设施建设
2016.12.27	《国家网络空间安全战略》
2017.6.15	工信部《工业控制系统信息安全事件应急管理工作指南》

资料来源：工信部，公安部等，东兴证券研究所

工控安全市场迈向成熟，增速超过 30%：2014 年 12 月我国已经发布《工业控制系统信息安全》国家标准，随后工控安全市场迅速发展。根据工信部电子科学技术情报研究所发布的《2013 年中国工业控制系统(ICS)信息安全市场研究报告》显示，2012

年国内工控系统信息安全市场已达 11 亿。另据工控网预测，中国工控系统安全市场 2015 年超过 20 亿人民币，将以每年超过 30%的复合增长率增长。目前电力行业由于涉及发电、输配电、用电等一系列的领域，对于通信网络具有充足的应用需求，因此是工控系统信息安全的第一大应用市场。油气石化、化工等行业自动化普及应用程度较高，为第二、三大应用市场。轨道交通等基础设施建设行业投资很大，且关系民生安全，因此为第四大应用市场并且规模增速高于其他行业。

图 30：工业控制系统信息安全管理系统

资料来源：启明星辰、东兴证券研究所

4.2.4 5G 部署将进一步扩大网络攻击范围

2018 年，5G 网络基础设施项目的陆续部署，虽然 5G 网络、5G 手机以及其他 5G 设备的部署仍旧需要耗费大量时间，但 2019 年毫无疑问将成为 5G 加速发展的一年。IDG 将 2019 年称为 5G 元年，并预测 5G 以及与 5G 相关的网络基础设施市场将从 2018 年的 5.28 亿美元，增长至 2022 年的 260 亿美元，年复合增长率为 118%。

5G 的转变将催生全新的运营模式和架构，这也会催生新的漏洞。会有越来越多的 5G 物联网设备直接连接至 5G 网络，使设备更容易遭到攻击，在云端备份或传输数据情况也会为攻击者提供大量的新的攻击目标。

4.2.5 人工智能、大数据与网络安全结合构建安全大脑

用数据驱动安全大脑，用安全大脑驱动安全构建多级网络安全监测平台，形成新体系。“数据驱动安全”的技术理念，以攻防技术研究为基础，利用大数据技术和威胁情报构建以检测和响应为核心的积极防御能力。

以数据安全为主要场景，依托安全大脑，发展第三代“查行为”的网络安全新技术。从关注样本黑与白上升到关注网络行为。白名单只能作为参考依据，而不再是无原则的信任清单。第三代技术突破了终端和边界的限制，通过尽可能全地收集大数据，安全大脑对每个样本 ID、IP、流量进行计算，判断行为是否合法，把可疑行为找出来告警，行为分析至关重要。

围绕“人是安全的尺度”，形成人+安全大脑协同运营的新方法。网络安全的本质是人与人之间的攻防对抗，及时告警、快速响应是网络安全核心问题，需采用“人+安

全大脑”的方法。借助人工智能、安全大脑争取 100%的检出率和零漏报率。

把安全能力分为三种：高位能力、中位能力和低位能力。安全大脑是高位能力，安全管理中心是中位能力，软硬件安全设备是低位能力。“三位能力”立体联动攻克网络攻击。

4.3 网络安全需求多个维度同时增长，带来网络安全市场的指数型增长

1）在同一个行业，随着核心业务互联网化程度提高，网络安全需求越来越刚需 / 持续增长；

2）随着传统行业逐个被互联网化，越来越多的行业需要网络安全 / 加速增长；

3）随着联网设备（除 PC 与服务器外，手机、物联网设备、车联网、工控设备联网、云基础设施）与设备智能化的爆发式增长，网元设备指数级增长，网络安全需求随之爆发式增长；

4）随着网络安全法规、政策的出台，新的安全领域与安全需求不断出现；

5）随着数据资产化、货币数字化，黑产对此更有兴趣，网络安全问题带来的经济损失指数级增长，网络安全需求随之指数级增长，2017 年和 2018 年，每年被盗的数字货币超 100 亿。

6）国际形势紧张、经济下行，网络间谍和网络犯罪会更猖獗。

六大维度同时增长，导致安全预算、安全市场指数级的增长。尤其 2018—2020 年这三年间，是加速增长的拐点。从全球范围来看，过去 15 年网络安全市场增长很快，未来将呈现“加速”增长趋势：从 2004 年 35 亿美金到 2017 年 1380 亿美金，增长了 39 倍多，年复合增长率为 33%；按照这个速度，到 2021 年，网络安全市场规模将达到 1 万亿美金；然而，还是没有赶上黑产的增长速度，2021 年网络犯罪带来的经济损失将达到 6 万亿美金。

2018 年是中国网络安全市场的拐点。从中国来看，2012 年—2017 年是网络安全发展的第二阶段，发展速度较快，2018 年开始网络安全发展将更快，绝大多数安全公司的收入增长都在 50% 以上，有的创新型安全公司业绩更是 400—500% 的增长。

4.4 业务模式迎来转变，产品走向运维

网络安全产品分散化难以真正满足安全需求。目前，国内网络安全产品从防护环节上可以区分为电磁安全、网络安全、应用安全、数据安全、自主可控等多种产品，而仅从网络安全大类又可以分出六小类，每一类又有不同的产品。传统的政府及大型企业的采购中，大到集团公司小到部门，都可能需要针对单个产品进行单独招标，难以满足真正的安全需求。由于分散招标，很难形成各种网安产品的立体联动防御和大数据分析，网安公司也很难提供有效的整体安全服务。

表 8：网络安全产品体系复杂

网络安全						数据安全
安全网关	安全监测	安全对抗	安全审计	安全平台	内容安全	数据交换
防火墙	IDS	漏洞扫描	身份认证	SOC	舆情监测	数据恢复
UTM	IPS	APT	行为管理	态势认知	网监	数据加密
VPN	威胁情报	抗 DDoS				电子取证

资料来源：Wind、东兴证券研究所

图 31：信息安全产品结构及分类

资料来源：互联网、东兴证券研究所

从“产品模式”转向“运维模式”是新形势下的新需要。过去，传统的安全企业通常以一次性交付产品的形式为客户提供安全防护，但随着资产数量的逐渐增加、系统脆弱性的进一步暴露以及攻击目的复杂化，传统的产品交付模式已经不足以满足客户与日俱增的安全需求。

首先，主动式防御需要有由统一运维商打通部署的各种产品，分析采集各种数据，目前产品招标模式下无法实现；其次下游私有云化趋势明显，随着 IT 系统的变迁，安全同样需要服务化；最后，叠加客户自身业务联网后安全性更加重要，客户安全需求升级。因此，运营维护成为重中之重，目前行业发展正在从产品模式向运维模式过渡。

信息系统安全工程（ISSE）与安全运维息息相关。是发掘用户的信息保护需求并随后设计和实现信息系统的一门艺术和科学，在一定的经济成本和精心设计下，这些系统便能够安全地抵御其面对的各种攻击。

表 9：信息系统安全工程（ISSE）过程

步骤 1	发掘信息保护需求（发掘需求）
步骤 2	定义系统安全要求（定义系统要求）
步骤 3	设计系统安全体系结构（设计系统体系结构）
步骤 4	开展详细的安全设计（开展详细设计）

步骤 5	实现系统安全（实现系统）
步骤 6	评估信息保护的有效性（评估有效性）

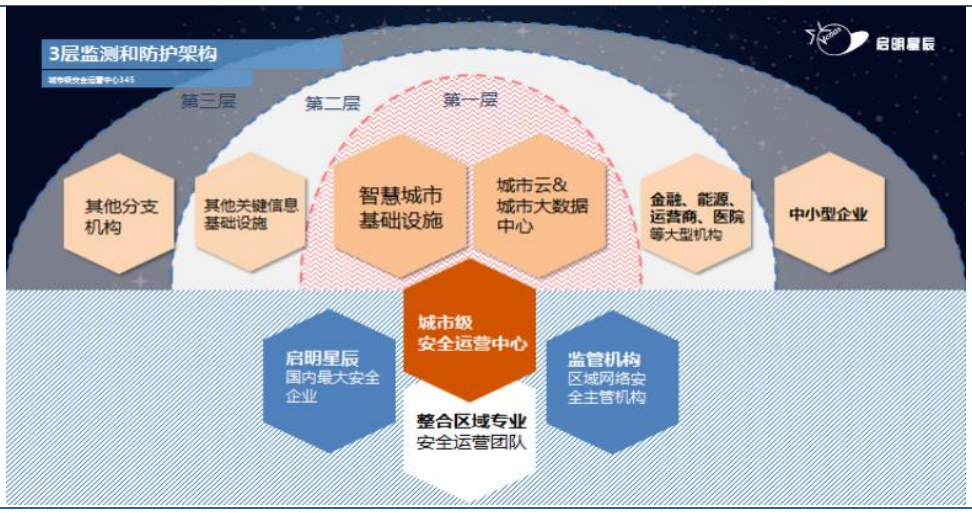
资料来源：互联网、东兴证券研究所

■ **政府安全运维市场：**

随着各地智慧城市的大力投入，政府对智慧城市带来的安全问题越来越重视。一些企业已经率先提出了“城市级安全运营”模式，其本质上是地方城市的安全托管云，以云的模式帮助各地智慧城市做安全态势感知等。按照分层的功能来看，第一层是智慧城市基础设施和城市大数据中心的监测和防护架构；第二层是其他关键信息基础设施以及金融、能源、运营商、医院等大型机构；第三层则是其他分支机构及中小型企业。

根据国家统计局的数据，我国目前省会级区划数 34 个，地级区划数 334 个，县级区划数 2850 个。按照市场成熟后，省会城市 5000 万规模，地级区划数（除省会外）2500 万规模，县级区划数 250 万规模计算，则智慧城市运营市场空间约为 160 亿左右。

图 32：城市级安全运营中心



资料来源：启明星辰、东兴证券研究所

■ **企业安全运维市场：**

企业网络安全投入占比大幅提升，有望进入全面运维期。央企长期以来缺乏安全运维服务，而随着企业信息化程度的逐步提高，关系国计民生的重要支柱型央企的数据资产重要性不言而喻，对安全运维的需求也迫在眉睫。

4.5 行业内整合趋势进一步增强，军民融合步入深水区

4.5.1 行业进一步整合，高动能、强风力、长周期和巨头诞生

我国网络安全行业整合趋势不断增强，联盟、协作共同体相继成立，企业间合作日趋紧密。一是大型 IT 厂商推进安全联盟建设，打造协同联动的网络安全防御生态。2018 年 3 月，华为联合天融信、微步在线、远江盛邦等厂商成立安全商业联盟，旨在通过创新架构深度整合联盟伙伴优势产品，实现终端、网络、应用等层面协同联

动，构建全网协同立体防御体系。8 月，腾讯携手卫士通、立思辰等 15 家上市企业，成立 P16 上市企业协作共同体，将深化沟通合作，在应对网络安全威胁、加强基础设施建设、掌握关键核心技术、引领网络安全产业的发展和生态环境的构建发挥重要作用。 二是云安全成为企业间合作的重点领域。浪潮与天融信、瑞星等安全企业携手共建云安全，例如天融信虚拟化安全防护系统、瑞星虚拟化系统安全软件实现与浪潮云海服务器系统兼容。

中电科集团根据国家安全战略发展需要，汇聚内部资源重点打造了网络安全子集团，并于 2015 年 5 月 8 日成立中国网安，包含上市公司平台卫士通，形成了完整的网络信息安全产业链，并积极寻求外部收购以图建立网络安全产业优势做大做强。

高动能。首先是国家安全的推动，没有网络安全，就没有国家安全，网络空间已经成为了大国角力的新战场；其次是在第四次工业革命的推动下，工业生产的个性化定制、网络化协同，产品与服务的网联智能，都把网络安全推到风口浪尖，以往买东西只衡量性价比，以后买东西要安全第一；还有产业强制性法规的推动，比如今年 5 月，欧盟的《通用数据保护法案》（GDPR），我国的《网络安全法》、《关键信息基础设施安全保护条例（征求意见稿）》等法律法规的实施。

强风力。企业不断提高网络安全在 IT 支出占比是市场扩大的推手。全球平均为 3.7%，美国是 4.8%，中国是 1.1%，我们和美国相差 4 倍。其实，重要的企业，国家关键基础设施的网络安全投资占比远远高于这个比例，达到 10%以上。如果未来网络安全在 IT 支出占比进一步提升，年增长率保持在 30%左右，每三年市场就会翻一番，十五年后就是三十二倍，按照现在 350 亿的基数，未来就是近万亿的市场。

长周期。第四次工业革命将带来机遇以及长周期的高速增长。第一次工业革命是蒸汽机的发明，机器替代了手工，风力持续了 80 年；第二次工业革命是电力的发明，小型自动化的机器替代了大型机器，风口同样持续了 80 年；第三次工业革命是计算机的发明，标准化的流水线诞生，自动化代替了电气化，风力持续了 60 年。现在第四次工业革命刚刚起步，可以判断风口行业至少将保持几十年的高速增长。未来我国网络安全行业也将出现巨头公司。

4.5.2 网信军民融合：市场和战场因网络互联、因融合而发展

作为军民融合的重点和前沿领域，网信军民融合正在成为热点。在可融合行业领域，高质量发展和深度融合具有线性关系，即融合的越深入，发展的质量也会越好。市场与战场、生产力与战斗力同一化，是接近于单一融合产物的深度融合，其核心理念是以市场和战场协同为并轴定向，以生产力和战斗力互促为双轮驱动，在能力界面上切实提升网信军民融合高质量发展，确保国家安全和利益。

市场交利、战场角力，原本是人类社会以楚河汉界划分的两个不同领域。但是网络通联了世界，使得人民生产生活的经济市场，日益成为国家博弈和军事慑战的一线战场。金融、能源、交通等战争潜力网的军事目标规划，更是彻底模糊了市场和战场的边界，甚至西方强国还将其列为最高军事效益的目标首选。现在的中国已经到了以民养军的重要阶段，主要体现在三个方面：

一是武器装备输出的养力。作为制造大国，必须注重国防基础工业和先进制造产业，能够随时将工业产能转化成战争动能，源源不断地制造出“杀手锏”武器装备。二是文化产品输出的养神。部队的熔炉文化在网络社会面临很大挑战，手机微信等社会媒体已经成为三军将士的精神家园。军队文化植 入的是战斗精神，而常态的文化修养和道德培育，必须由市场提供优秀的影视作品来完成。三是联勤保障输出的养生。随着国防和军队改革，社会化联勤保障体制逐步建立并且常态运行。市场只有提供可靠的、安全的、符合要求的各种商品，才能够使得部队将所有精力都放在谋打赢的军事斗争准备。概括地讲，就是**市场要向战场提供硬通货**。

5. 投资建议

中美网络攻防能力差距较大，政策战略加快部署利好网络安全行业。全球网络空间呈现对抗公开化、力量专业化、部署攻势化的趋势，以战略网络战为代表的网络空间军事手段异军突起。网络安全攻防，防御成本急剧上升、碎片化安全问题严重，国际网络空间竞争博弈进入深水区。美国国家级攻防对抗将成为新常态，在网络空间司令部、“网络航母”、网络空间攻防能力、攻击装备上均一马当先，我国网络安全面临高压态势。我国网络空间防御能力严重滞后，未来国家战略政策加快推进有助于国内网络安全行业的进一步整合发展。

美国火眼并购建立综合安全管理平台，军民融合、政企合作具有借鉴意义。火眼在 APT 防御、网络安全服务生态系统领域独步武林，通过并购实现在安全服务领域较大的跨越，搭建起了以侦测、响应、情报、咨询为一体的综合安全管理平台。

网络安全行业加速增长，行业技术发展催生更大市场需求，业务模式转向运维。数据资产急速增长，传统边界安全转向内容安全和数据安全；云安全带来虚拟化需求，成为云-网-端立体式安全核心；物联网安全和工控安全兴起、5G 部署将进一步扩大网络攻击范围，催生新的防御需求。

随着等保 2.0 的临近，网络安全产业市场空间进一步增加，网络安全行业整合趋势进一步增强，中美贸易冲突下国家队将充分受益，重点推荐卫士通。公司作为我国密码技术方面的龙头企业，在密码产品多样性和密码算法高性能实现方面一直保持国内领先水平，具备渠道和商业模式两方面的优势，形成了以“安全咨询、安全评估、安全建设、安全运维”为主要内容的信息系统全生命周期安全集成与服务能力。伴随云计算、5G 应用场景、量子通信带来的更多安全挑战，网络信息安全领域未来市场空间更为广阔。5G 安全业务明年有望达到 5 亿级别，打开公司估值空间。与阿里打造“ 网安飞天云”云平台，未来党政军自主可控安全云平台中取得更大市场份额，成为公司未来成长支柱之一。卫士通大股东中国网安布局、开展量子密码的相关研究，在量子加密方面走在世界前列，量子通信行业发展前景广阔长期市场规模将超过千亿。

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。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。在金融领域、移动互联网领域、云计算领域加快部署。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，卫士通还积极布局安全支付手机市场。

与阿里云合作，卡位党政军云安全。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，并与中国最大“阿里云”合作，打造“网安飞天”安全云，有望在安全集成领域掀起另一轮高增长态势。在云计算领域，打造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。包括主动防御（基于态势感知的网站防护服务）、身份安全、安全移动办公。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。

卫士通有望在军工业务中获得未来新一轮增长极。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。同时，卫士通在量子加密领域加快布局研发，公司大股东中国网安已布局、开展“量子密码” 的相关研究，公司有望竞争量子通信未来长期千亿市场空间。

我们预计卫士通在 2019 年迎来业绩拐点。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。

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 1：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。