东兴证券 DONGXING SECURITIES

助力网军建设，网络战争时代的反导系统

——卫士通（002268）深度报告系列之六

2019 年 04 月 01 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

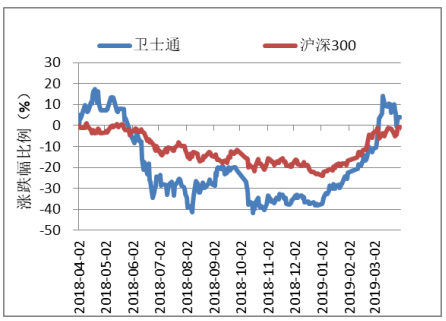
010-66554018 Zhangzq_yjs@dxzq.net.cn

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）	229
流通市值（亿元）	222
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：

网络战是信息时代核武器，我军军改重点关注网络攻防领域。网络空间被誉为国家的第五空间，其安全性关系着国家的稳定与发展。美国政府著名智囊兰德公司早在 2009 年就表示，网络战是信息时代的核武器，因为网络攻击会直接威胁现代社会赖以运转的信息存储与控制机制，其威慑程度甚至远远超过原子弹。此前虽然我军拥有负责网络攻防的部门和技术人员，但这些力量分散于各个总部、军兵种和军区之中，缺少了由统一协调和技术规模效应带来的作战能力提升，此次军改将网络攻防作为战支下辖的重点建设领域，足以看出我国网络安全在国家安全领域的重要地位。

美军网军建设世界领先，网络靶场和网络武器库是网军建设关键配件。与其他作战模式一样，网络战同样需要武器装备的研发，同样需要有专门的训练环境进行军事演习和装备测试。美网军发展之所以领跑世界，除在部门、组织、机关设置方面具有前瞻性外，更多的依赖于其在网络安防领域中训练体系的科学性和基础设施的完备性。早在 2008 年 1 月，美国就启动了国家网络靶场项目（NCR），该项目建成后为美国国防部、陆海空三军和其他政府机构服务。与传统战争模式需要的坦克、飞机、舰船等武器类似，网络战同样需要武器来作为攻防的重要方式。目前美国已研发储备了两千余件电脑病毒武器，且逐级向着体系化的规模发展。

我军网军建设尚有不足，卫士通将是网络战时期的反导系统。此次军改从部门、机关设置上搭建起了我国网军的主要骨架，但在网络靶场以及网络武器库建设方面尚属于初期阶段，还有巨大的发展潜力和市场空间。卫士通背靠中电科集团，深耕网络安全领域多年，拥有国内顶级的信息安全资质，最强的信息安全研发团队，最完善的质量服务体系，网络安全理念、技术和产品均为国内顶尖；卫士通产品谱系齐全，应用广泛，满足服务范围广的要求；同时作为上市公司，卫士通具有拥有良好的资本平台，能够承受成本高昂的研发费用。卫士通将是网络战争时期的反导系统。

公司在 2 月 28 日电科投资完成增持 1.08 亿。公司 2019 年几大新业务进入收获期，管理层大换血值得期待。我们预测公司 2019 年~2020 年利润分别为 5.47 亿、8.07 亿，EPS 分别为 0.65 元、0.96 元，维持“强烈推荐”评级。

风险提示：网军建设进度低于预期。

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	1,931.00	5,226.90	7,691.92

增长率（%）	12.21%	18.80%	-9.64%	170.68%	47.16%
净利润（百万元）	155.75	169.05	139.95	547.30	807.85
增长率（%）	4.69%	8.54%	-17.22%	291.08%	47.61%
净资产收益率（%）	10.46%	3.94%	3.19%	11.47%	15.16%
每股收益(元)	0.36	0.21	0.17	0.65	0.96
PE	76.23	130.16	164.43	42.05	28.49
PB	7.97	5.36	5.24	4.85	4.38

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

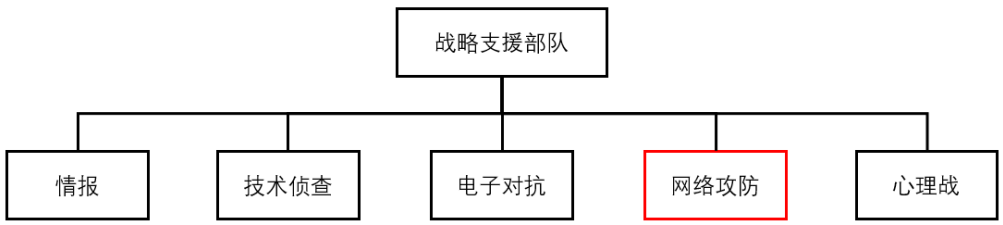
1. 网络安全部队异军突起

1.1 军改突出网络安全领域为国防重点领域

随着军改完成，我军从军委领导下的总部负责制转变为军委领导下的多部门制，在军种设置方面也做出了巨大调整，其中战略支援部队作为新设置的军兵种首次出现。战略支援部队主要的使命任务是支援战场作战，使我军在航天、太空、网络和电磁空间战场能取得局部优势，保证作战的顺利进行。战略支援部队可能包括情报、技术侦察、电子对抗、网络攻防、心理战五大领域，它是联合作战的重要力量，将与陆军、海军、空军和火箭军的行动融为一体，贯穿整个作战始终，是战争制胜的关键力量。

其中专门负责网络攻防的相关单位及其人员，从实质上来说就是我国对标其他军事强国网络部队的“网军”。

图 1：战略支援部队五大任务领域



资料来源：百度百科、东兴证券研究所

此前虽然我军拥有负责网络攻防的部门和技术人员，但这些力量分散于各个总部、军兵种和军区之中，缺少了由统一协调和技术规模效应带来的作战能力提升，此次军改将网络攻防作为独立概念重点建设，足以看出我国网络安全在国家安全领域的重要地位，也意味着我军将在网络安全领域集中力量和投入打造出一支足以匹配其他细分军兵种地位的新兴作战力量。

1.2 组建专门网络攻防力量是合理性和必然性的结果

网络空间被誉为国家的第五空间，其安全性关系着国家的稳定与发展。从国际角度看，当前网络空间安全形势严峻，从个人信息泄露、勒索病毒爆发，到俄罗斯黑客影响美国大选、乌克兰因为黑客攻击大规模停电事件，凸显出网络安全已经从影响个人信息安全发展到了组织间，国家间的斗争，从个人兴趣爱好发展到了团队以营利为目的，甚至是带有政治色彩的较量。

1.2.1 网络战是信息时代的核武器

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。

美国政府著名智囊兰德公司早在 2009 年就表示，网络战是信息时代的核武器，因为网络攻击会直接威胁现代社会赖以运转的信息存储与控制机制，其威慑程度甚至远远超过原子弹。1. 网络战威慑范围更大。目前一枚能量最大的核弹摧毁范围有限，但一次网络攻击，理论上可以瘫痪一个国家、甚至整个世界；2. 网络战威慑效果更强。网络战不仅可以在网络空间制造混乱，也可以通过控制攻击实体空间，其匿名性也将使威慑报复陷入混乱；3. 网络战威慑实施更快。一个网络天才能够“一键敲击、全球到达”，瞬间发动一场致命的网络攻击，无需核弹打击需求的运载工具；4. 网络战威慑方式更多。对一个国家政权来说，网络战不仅可以实施攻击瘫痪其民生基础，而且能够通过思想殖民颠覆其国体政体。

1.2.2 我国遭受网络攻击情况严重

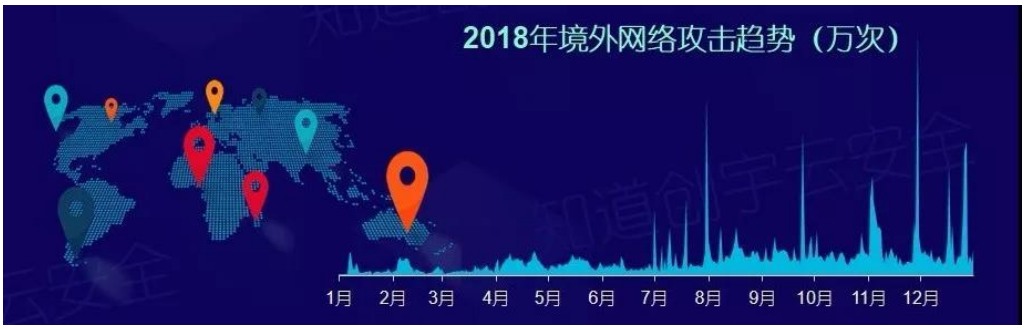
以 2018 年我国互联网遭受 DDoS 攻击规模为例，其中中型 DDoS 攻击（10-50Gbps）更是惊人地增长了 293.44%，而超大型攻击（600Gbps 以上）的增长率也已达 93.33%。中国依旧是全球遭受 DDoS 攻击最严重的国家。就全国范围来看，攻击仍然集中于互联网经济较为发达的地区，如广东、浙江、江苏等地，严重威胁了我国的互联网安全。

图 2：我国遭受网络攻击十分严重

资料来源：《2018 年度网络安全态势报告》、东兴证券研究所

而其中 3.26%的 Web 攻击发起地域源于境外，且总体呈现平稳上升的攻击态势，平均每日攻击量数千万次，并伴有多次大幅波动。大部分攻击来自美国、韩国及日本等，其中美国一直以来都是最大的境外攻击源头。需特别注意的是，来自境外的攻击中，针对政府和金融网站发起的攻击次数远高于其他网站。可见来自境外的网络攻击目标的带有明显的政治色彩。为维护政府的正面形象，及保障金融网站的重要资产，需要建立完善且牢固的网络安全体系来保证网站的安全稳定运行。

图 3：我国遭受境外网络攻击严重



资料来源：《2018 年度网络安全态势报告》、东兴证券研究所

为应对网络攻击，根据北约颁布的《国家网络安全框架》，目前世界上已有一百多个国家具备一定的网络空间攻防能力，公开发表网络安全战略的国家和地区近 60 个，且数量仍在不断增长中。

表 1：各国网络安全力量建设情况

国家/地区	建设情况
英国	2009 年 6 月出台首个国家网络安全战略，并宣布成立两个网络安全新部门，即网络安全办公室和网络安全行动中心，分别负责协调政府各部门网络安全和协调政府与民间机构主要计算机系统安全保护工作。
俄罗斯	上世纪 90 年代就设立了信息安全委员会，专门负责网络信息安全；2002 年推出《俄联邦信息安全学说》，将网络信息战赋予了极高的地位，比作未来的“第六战争”。
北约	2008 年 5 月，爱沙尼亚、拉脱维亚、立陶宛、德国、意大利、西班牙和斯洛伐克签署协议，将共同出资建立一个反网络攻击研究中心，以提高防御网络攻击的能力。
以色列	在 1998 年就将成功入侵美国防部网络的青年招入部队，并开始加大对网络作战的研究力度。
韩国	在 1999 年 3 月的总统业务报告中提出，从 1999 年起到 2015 年为止，分 3 个阶段确立国防信息化的目标，首先对信息组织进行统一调配，并建立信息通信网，以应对网络战。从 2000 年开始，韩国每年的国防预算有 5%专门用于“提高应对信息战的核心技术”。2003 年 11 月成立国防信息战中心。
印度	目前建立了海陆空三军联合计算机应急分队，在位于新德里的陆军总部建立了专门负责网络中心战的网络安全部门；2009 年印度陆军决定将网络安全能力延伸到印军师一级；2010 年 4 月印度国防部高级官员宣称，印度已经决定成立网络防御司令部，以保护政府和军用网络的安全。
日本	日本防卫厅根据其 2005-2009 年《中期防卫力量发展计划》，组建一支由陆海空自卫队参加，人数多达 5000 人的“网络部队”；日本众议院已通过《自卫队法》修正案，“以应对未来弹道导弹、网络战等多种威胁”。
德国	2009 年 1 月，德国内阁批准了一项旨在“加强联邦政府信息安全”的法案。德

	国联邦国防军正在训练自己的网络战部队，陆军准将克里塞尔将率领总数为 6000 人的部队——“信息和网络技术管理部”，主要应对网络突发情况，主要针对有关外部服务器和网络的攻击。
朝鲜	在人民武力部总政治局下设了 121 部队，履行扰乱对方指挥通信网、破坏网站等网络系统的实质性的网络战。
英国	2018 年根据英国媒体报道，英国将成立一支 2000 人的网络部队，以提升其网络战的能力。这支部队将在近期内宣布成立，其规模是英国目前网络部队人数的近四倍。网络部队将由英国政府通信总部（GCHQ）官员、军事人员和承包商组成，并将获得政府 2.5 亿英镑以上的资助。

资料来源：《网络战成就新一轮全球军备竞赛》，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	成立时间	国家	部队
2009 年	美国	网络战司令部	2005 年	印度	网络部队
2014 年	俄罗斯	网络战司令部	2013 年	日本	网络空间防卫队
2014 年	日本	网络安全战略本部	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

1.3 美国网军建设领先世界

在网络部队建设领域中，美国起步最早，建设最为成熟，作战经验最为丰富。早在 1991 年海湾战争期间，美向伊拉克派出特工（实际上是网军），将伊拉克从法国购买的防空系统中使用的打印机芯片，换成含有计算机病毒的芯片。在美对伊实施战略空袭前，致使伊拉克防空指挥中心主计算机系统程序错乱、C3I 系统失灵。这次行动打开了世人的眼界，使人们开始重视网络战。 从 2010 年率先建立网络空间司令部，到 2013 年公开承认建有专司“进攻”任务的网络战部队，从 2011、2015 年国防部接连发布两份网络空间战略文件，到网络安全国防预算持续攀升，再到最近的 2020 国防预算计划，美国的网军建设始终是国际社会关注焦点。

1.3.1 美军网络战三部曲

美国政府网络安全战略演进经历了 3 个阶段，与此同时，美军网络战力量建设也完成了从国内防御到全球攻击的布局。

在力量布局方面，美军已完成了从国内防御到全球攻击的演进。

克林顿时期政府时期，美国网络空间安全战略“浮出水面”，美军主要进行网络防御。1993 年克林顿政府首次提出建设“国家信息基础设施”。1998 年，克林顿颁布 63 号总统令，首次提出“信息安全”概念。同年，美国国防部正式将信息战列入作战条令，并批准成立“计算机网络防御联合特种部队”，专司军事信息网络防御。

小布什政府时期，美国网络空间安全战略“加速发展”，美军扮演着“以攻验防”的角色。“9·11”事件后，布什政府把加强网络信息安全和防范网络恐怖主义作为头等大事。2003 年 2 月，美国发布第一份专门针对网络空间国家安全的战略报告《网络空间安全国家战略》。

2005 年，美军组建专门负责网络战的“网络战联合构成司令部”。从 2006 年起，美国每两年举行一次“网络风暴”演习，以全面检验国家网络防御水平和实战能力。演习中，由美军网络战专业力量担任“蓝军”，承担演习中的网络攻击任务。

奥巴马政府时期，美国网络空间发展战略“基本成型”，美军网络战力量加紧在全球布局。2009 年，奥巴马上台伊始，立即开始了为期 60 天的信息安全评估，随后出台一系列战略报告。值得关注的是《美国网络空间国际战略》，它成为美国处理网络问题的“指南针”和“路线图”。美国国防部紧接着出台《美国网络空间行动战略》，强调将与盟友和国家伙伴合力加强集体网络安全，具体行动体现在两个方面。

一方面，美军加快开发全球作战的网络武器。2010 年 7 月伊朗核核设施遭到“震网”病毒攻击，导致 1/5 的离心机损毁，核计划被迫延期；2012 年 5 月威力巨大的网络攻击病毒“火焰”现身，俄罗斯杀毒软件厂商卡巴斯基指出，有证据显示，“火焰”与“震网”同宗同源。2014 年，美国国防部又启动了网络战武器研发的“X-计划”，开始开发全球感知、全球攻击、全球反制的网络战武器，美军网络战的触角已经延伸到全球网络空间。

另一方面，美军大规模扩编全球作战的网络攻击部队，2012 年 3 月 24 日，美《防务新闻》周刊网站发表主题为《美国采取网络攻势》的文章称，美军网络空间司令部正在所有 6 个地区战斗司令部成立网络战小组。2014 年年初，美军将网络空间司令部由 900 人扩编到 4900 人，并建立“国家任务部队”、“作战任务部队”和“网络保护部队”，明确了协助海外部队策划并执行全球网络攻击任务。随后，美军网络空间司令部司令亚历山大上将在国会又宣布拟成立 40 支网络战部队，承担在全球范围内进行网络攻击的任务。2016 年，美国防部发表声明称美军网络司令部下属的 133 支“国家网络任务部队”已经全部具备初步作战能力。2017 年，美国总统特朗普宣布，将美军网络司令部升级为一级联合作战司令部，从而使美军联合作战司令部由 9 个变为 10 个。从而，美国网络部队将形成“总统-国防部长-网络司令部”的网络战指挥机制。美军网络战力量已经从作战武器、作战任务到力量部署，实现了全球网络攻击的力量布局。

表 3：美国网军建设主要时间节点

时间	法律法规
1993 年	克林顿政府首次提出建设“国家信息基础设施”。
1994 年	美国国防大学率先成立了旨在培养信息战人才的信息资源管理学院，首批 16 名学员被称为“第一代计算机网络战士”，他们的任务就是利用计算机在网络空间与敌人展开全面信息对抗。
1999 年	美国国防部批准联合作战司令部的调整计划，赋予航天司令部网络攻击和防御的职能，大

	力发展信息战进攻能力。
2002 年	布什总统在 2002 年发布了第 16 号“国家安全总统令”，组建美军历史上、也是世界上第一支网络黑客部队——“网络战联合职能司令部”（JFCCNW）。
2002 年	美国海军率先在弗吉尼亚比奇的小溪流两栖作战基地成立海军网络战司令部，统一指挥海军舰队信息战中心、海军网络和太空行动司令部及海军计算机网络防御特攻队等海军网络战单位。
2006 年	2006 年 11 月，美国空军宣布将成立网络战临时司令部。根据原计划，空军网络战司令部管辖 65 个网络战中队、预备役和国民警卫队，此外还有 4 个联队，包括大名鼎鼎的第 67 网络战联队。
2009 年	美国军方宣布了一个被称作“挑战网络”的系列网络竞赛项目，倡议书发布在白宫网站上，正式向美国年轻人发出号召：“学生黑客、骇客、极客们，山姆大叔需要你们。该系列赛包含三个针对中学生和大学生的全国计算机竞赛，旨在发现其中的网络奇才。竞赛将测试学生进攻防守数字目标、盗取信息以及追踪发现信息盗取者等技能。竞赛在 2009 年 5 月 29 宣布正式开赛，到暑假前结束。此次活动的目标是发现 10000 名网络人才。
2010 年	美国成立网络司令部，由刚晋升为四星上将的亚历山大全权负责。这支部队包括成千上万的国安局间谍以及 14000 名来自美国海、陆、空三军的网络司令部军人。这支网络部队将数字信息发展成一种新型武器，使其能够像常规的陆空支援一样向前线部队提供“网络火力支援”。
2010 年	美国国家安全局(NSA)美国网络部队的建设工程于 2010 年 5 月正式开工，耗资 32 亿美元，坐落于马里兰州的米德堡。这项代号为“M”、占地 227 英亩的工程包含一个 150 兆瓦特的变电站、14 栋行政大楼、10 个停车场以及冷却加热工厂。
2016 年	美国防部发表声明，美军网络司令部下属的 133 支“国家网络任务部队”已经全部具备初步作战能力，即能够“执行基本任务”，但“不代表做好了全面作战准备”。
2017 年	美国总统特朗普宣布，将美军网络司令部升级为一级联合作战司令部，从而使美军联合作战司令部由 9 个变为 10 个。从而，美国网络部队将形成“总统-国防部长-网络司令部”的网络战指挥机制。
2019 年	根据白宫对 2020 财年的预算要求，美国空军准备启动一项新的 3500 万美元的进攻性网络计划——“网络任务部队基础工具”，作为美国网络司令部总体计划的一部分，为美国空军网络任务部队提供先进的网络战能力。

资料来源：互联网，东兴证券研究所

同时，根据根据白宫对 2020 财年的预算要求，美国空军准备启动一项新的 3500 万美元的进攻性网络计划——“网络任务部队基础工具”，作为美国网络司令部总体计划的一部分，为美国空军网络任务部队提供先进的网络战能力。

该计划的主要内容：通过研究、开发、测试、评估、加速原型设计、演示和部署网络技术和能力等，开发一系列攻击性网络工具，使战斗指挥官在网络空间中作战时能够通过网络来操纵、破坏、拒绝、降级或破坏目标计算机、信息系统和网络。该计划特别强调网络工具的互操作性。在 2020 财年，美空军希望该计划能够扩展过去研究的

一系列网络基础工具，开发其他工具和软件，提供可与美网络司令部架构互操作的原型系统等。美网络司令部领导人也表示，相关军种将不再开发用于单个军种的烟囱式的工具或基础设施。

此外，预算文件还指出，攻击敌方网络、电话、综合防空系统，指挥和控制系统以及通过电磁频谱创建网络效应所需的工具,将纳入空军的分布式网络作战行动(DCWO)组合。DCWO 组合可以向战斗指挥官提供网络效应，包括环境的网络作战准备，攻击性网络反击、网络攻击、电子战作战、任务规划、情报、网络安全产品和服务以及指挥和控制/态势感知（C2SA)。

由此可见，美军在网络攻防方面的巨大投入，以及未来国家间网络战争的激烈程度。

目前美国网军已具备基本作战能力。纵观美国网络部队的发展历程，主要呈现出以下特点：

第一，网络部队任务网络防御为主逐渐向网络进攻转变，打造攻防兼备的网络作战力量。克林顿时期，美国高度重视本土的网络防御，网络部队以“防御”为主。“9·11”爆发后，美国网络反恐的压力增加。布什政府提出“先发制人”战略，着力发展美军网络部队攻击和防御能力，强调“攻防均衡”。自奥巴马上台后，美国即成立了网络司令部，开始大力整合网络部队，强化进攻能力。2015 年 4 月 23 日，美国发布新版网络安全战略，明确提出发展美国网络进攻能力。2016 年底，美国通过国防授权法，赋予了网络司令部更大的网络反制权，可以主动发起网络攻击。

第二，由各自分散作战逐渐转向跨区域联合作战，各军种网络部队融合程度加深。从海湾战争中的作战级“信息战小组”，到今天的一级联合作战司令部，从各军种独立的信息战部队，到今天统一指挥作战的网络司令部，美军网络部队的体系结构更加系统和优化。各军种网络部队从陆、海、空齐聚网络空间，相互之间协同作战，同时与其他作战部队之间联合作战，使美国网络作战行动高度统一。

第三，大力发展战术级网络作战单位。美国网络司令部下属的 133 支网络任务部队，分别承担具体的作战任务：国家任务部队主要保护美国国内电网、核电站等重要基础设施；网络保护部队主要保护美国国防部的网络与系统；作战部队主要执行网络攻击任务；支持部队为国家任务部队与作战部队提供分析与规划支持。

第四，各军种网络司令部均依托具体作战单位成立。美国空军网络司令部依托第 24 航空联队建立起来，陆军网络司令部依托陆军第 2 军建立，海军则以第 10 舰队作为网络司令部。这些单位既是司令部机构，也有具体的作战任务。

第五，美军网络部队与情报部门高度合作。首先，国家安全局局长兼任美军网络司令部司令。国家安全局作为美国的情报机构，主要负责外国情报搜集和“信息保障”。同时，国家安全局也具有推进网络作战行动的职能，其网络空间技术为美军网络部队提供了技术支撑。“蠕虫”“永恒之蓝”等威力巨大的病毒，无不出自国家安全局之手。其次，情报战也是网络战的重要形式之一。最后，美军美军网络部队的成员不仅是军内人员，还包括一些天才黑客、网络技术专家、情报部门专家等。

从以上特点可以看出，美军网络部队的最终发展目标是要提升其在网络战场的实战能力，保持美国的网络空间优势。可以预见，网络部队将成为未来战争决胜的关键因素。

图 4：美军网络司令部标志

资料来源：公司官网、东兴证券研究所

图 5：美国莱克兰空军基地网络战中心

资料来源：公司官网、东兴证券研究所

1.4 网络把场和网络武器库是网军建设的关键配套要素

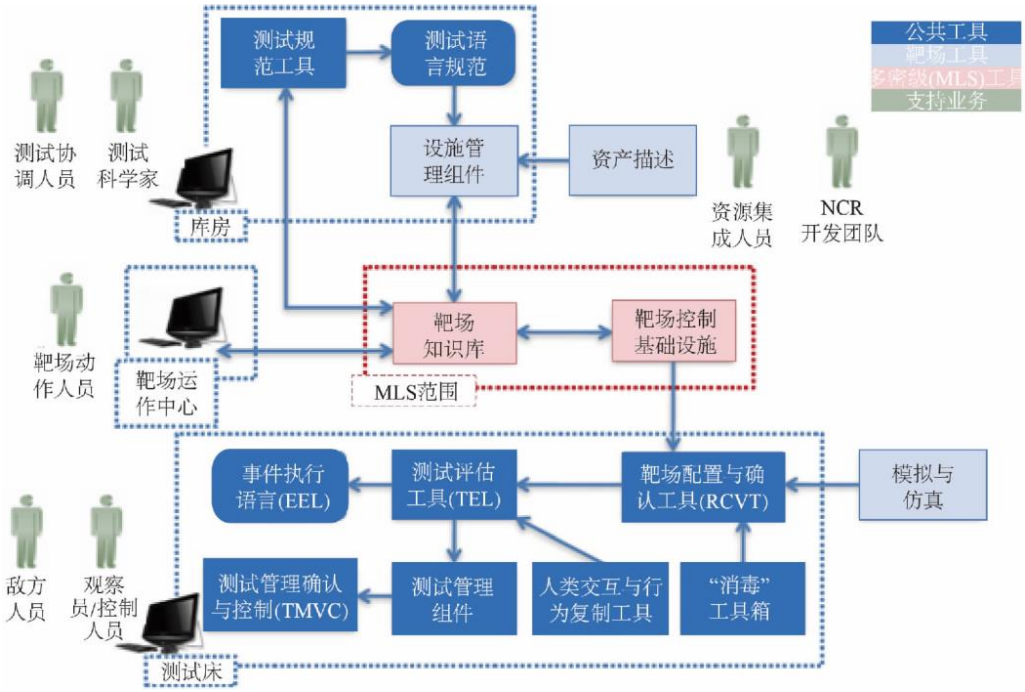
与其他作战模式一样，网络战同样需要武器装备的研发，同样需要有专门的训练环境进行军事演习和装备测试。美网军发展之所以领跑世界，除在部门、组织、机关设置方面具有前瞻性外，更多的依赖于其在网络安防领域中训练体系的科学性和基础设施的完备性。

因此网军建设除在军种、领导体系等顶层设计方面需要与时俱进外，作战训练，武器研发生产等具体事项也需要及时跟进。其中网络靶场和网络武器库建设这两项工程分别对应了网军日常的攻防训练和武器研发生产，应予以高度重视和大力投入。

1.4.1 网络靶场是网军作战训练，提升战斗力的重要基础设施。

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。

图 6：网络靶场原型系统体系结构



资料来源：《国家网罗靶场的建设与发展》、东兴证券研究所

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。同时网络战作战人员可以在靶场环境下反复训练各类网络攻击和防御的方式，并通过生成的报表日志来进行总结。

美国网军发展迅速很大程度上得益于其网络靶场建设良好。美军作为网络中心战的提出者，最早开始了网络靶场的建设，其军事网络靶场的建设体系最完整，技术最先进，应用也最成熟。早在 2008 年 1 月，美国就启动了国家网络靶场项目（NCR），该项目建成后为美国国防部、陆海空三军和其他政府机构服务。美国网络靶场的建设目标是提供虚拟环境来模拟真实的网络攻防作战，针对敌对电子攻击和网络攻击等电子作战的手段进行试验，以实现网络空间作战能力的重大变革，打赢网络战争。

图 7：美军网络靶场训练

图 8：美军网络靶场训练

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

美国国家网络靶场（NCR）建设主要分为四个阶段：第一阶段主要进行靶场的初步概念设计，形成详细的工程计划和系统演示验证计划，制定实施方案；第二阶段则进行靶场的关键技术评估，系统研制开发和原型构建；第三阶段则进一步完善基础设施，进行初步测试，使靶场可以进行交付使用；第四阶段则针对具体项目进行网络实验。

在网络创新和发展速度极快情况下，网络靶场后续的更新、维护和升级更为重要。目前美国国家网络靶场（NCR）由洛克希德·马丁公司负责维护升级。2018 年 2 月美陆军司令部对洛马公司授出一份总价值 3390 万美元的合同，内容为洛克希德·马丁下属的导弹与火控系统分部与将为美军国家网络靶场（NCR）进行一系列例行维护和能力提升项目，旨在使国家网络靶场具备测试和验证更先进的网络战技术的能力，相关工作已按计划展开；根据合同要求，洛·马公司将对国家网络靶场的现有能力进行深度升级和大幅扩展，能够演示和研究目前最具破坏性的网络病毒以及隐蔽性最强的恶意代码，同时将其传播有效控制在靶场范围内，避免向公用或军用网络泄漏。

除国家级网络靶场外，军用或某些专业领域的网络靶场也有建设的需求和必要。在美国最大的美国国家靶场（NCR）建设之前，美军已陆续建设了国防部信息确保靶场（DoD IAR）、联合网络空间作战靶场（JCOR）、海军网络空间作战靶场（NCOR）、联合信息作战靶场（JIOR）、战略司令部网络作战靶场（SCOR）、陆军国民警卫队增强型网络训练模拟器靶场（AR-GENTS）等多个军事网络靶场。

表 4：美国部分军用网络靶场及职能

国家/地区	建设情况
IAR	2009 年 10 月建成并投入使用，由美国国防部信息系统局安全作战室倡导建设，实际运营为海军陆战队司令部。IAR 旨在提供一个全球信息栅格（GIG）作战仿真环境，其信息保障、网络防御能力以及网络服务均处于封闭环境中。IAR 也是国防部网络人员的虚拟训练场，为网络演习、新信息保障技术与网络防御战术、技术和规程的测试与评估提供综合仿真环境。
JCOR	联合网络空间作战靶场可以用于网络实兵训练以及虚拟仿真训练靶场，现在增加了攻击性作战训练。不断变化的任务还包括支持动力学事件的网络作战训练。美军将联合网络空间作战靶场描述为一个靶场联盟，其主要成员还包括海军网络空

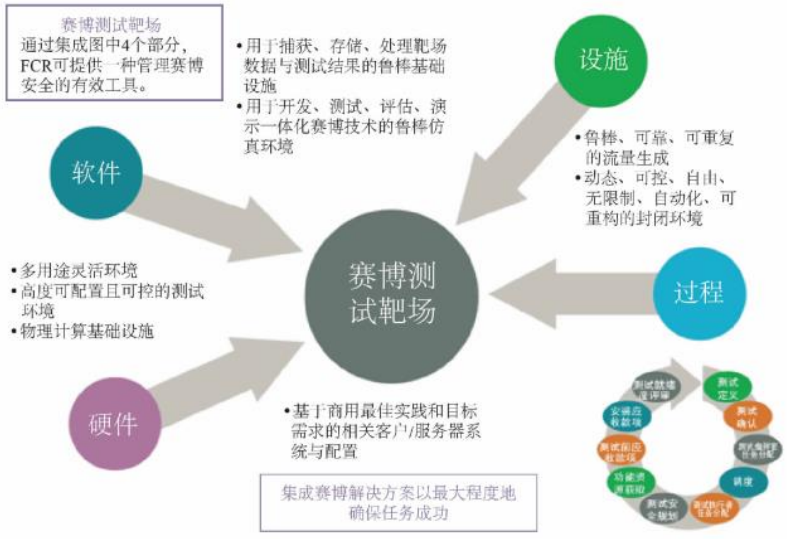
	间作战靶场、战略司令部网络作战靶场以及陆军国民警卫队增强型网络训练模拟器靶场等。
NCOR	目前主要用于测试商业和定制开发的安全应用程序，如基于主机的安全系统、海军“红队”和“蓝队”工具包等。
JIOR	靶场构成了与实弹发射相关的逼真网络空间环境，支持各作战司令部、各军种和国防部各机构以及试验界在信息作战和网络空间任务领域的训练、试验和实验。靶场可以进行战术、战役和战略级训练和试验。除了国家实验室、工业界和学术界之外，靶场可以与美国国防部以及各军种的网络靶场连接。靶场的主要任务是在采办周期中对指挥和控制技术设备进行试验。

资料来源：《网络战成就新一轮全球军备竞赛》，东兴证券研究所

此外在非军事领域，云计算、大数据、移动互联网和物联网等技术在生产活动中扮演的角色越来越重要，因由此诞生出了一批非军用工业级别靶场，如 2013 年，美国国家能源部发起并实施了“国家 SCADA 测试床项目”（NSTB）。任务是测试现有的和新研发的设备和系统，研发安全架构设计和新技术；NSTB 项目由爱达荷国家实验室（INL）和桑迪亚国家实验室（SNL）联合管理和领导，联合国家实验室、工业企业、行业协会、私营企业，帮助电力、石油和天然气能源部门识别和解决 SCADA 和控制系统的脆弱性漏洞问题，共同推动网络与信息系统的信息安全研究工作等。

英国国家级网络靶场的建设稍晚于美国。2010 年 10 月英国国防部相关人员宣布成立英国联合网络靶场。联合网络靶场可以与其它网络设施进行组网，而且是英国第一个可以用于商业用途的网络靶场。该联合网络靶场可以为网络行动提供高度可控的测试和训练环境，并通过可配置的网络体系结构来开展通信，其结构支持动态、常规和核心的企业服务。联合网络靶场还能够安全地演练网络攻击和防御， 并可测试新的以及现有的网络软硬件。

图 9：英国联合网络靶场的组成及主要功能



资料来源：《国家网罗靶场的建设与发展》、东兴证券研究所

从美、英两国的网络靶场的建设中我们可以归纳以下几点：

1. 重点网络靶场的建设多由国家级安全部门牵头；2. 网络靶场一般有多个层级，最上层级为国家级的联合网络靶场，适用范围大，内容涵盖广，用户种类多。而次级靶场如军用或某些工业领域专用靶场在特定内容和适用领域有所突出，强调专业性；3. 网络靶场的建设、运营和维护多采取出军民融合的模式，大部分都交给网络安防领域实力强大的军工或专业软件企业负责。

1.4.2 网络武器库是网络攻防战中成败的关键所在

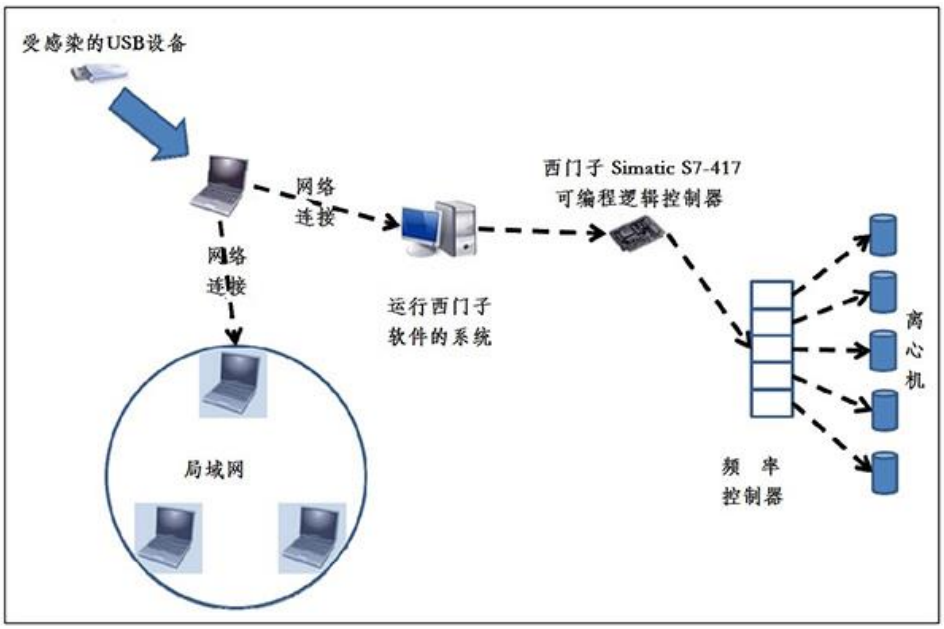
与传统战争模式需要的坦克、飞机、舰船等武器类似，网络战同样需要武器来作为攻防的重要方式。目前美国已研发储备了两千余件电脑病毒武器，且逐级向着体系化的规模发展。这些电脑病毒武器分属不同用途种类，如网络情报站武器、网络心理战武器、网络阻瘫战武器等。

在 2016 年 G20 峰会上，前美国总统奥巴马称美国拥有全球最大最好的网络武器库，称：“我们正在进入一个新的时代，这个时代里，很多国家都拥有强大的（网络）能力。老实说，我们（美国）比其他任何国家都更有实力，无论攻击还是防御方面。”2017 年 5 月 12 日，全球多个国家的网络遭遇名为“想哭（Wanna Cry）”的勒索软件攻击，据统计，涉及中国、英国、西班牙、俄罗斯等上百个国家和地区。电脑被勒索软件感染后文件会被加密锁定，支付黑客所要赎金后才能解密恢复，受攻击对象甚至包括医院、高校等公益性机构，后续有报道指出该勒索软件为黑客组织从美国国家安全局（NSA）的网络武器库盗取而来。

目前大家耳熟能详的网络战病毒有“震网”(Stuxnet)病毒、“Fanny”蠕虫病毒、“Regin”隐形间谍软件、“硬盘固件”病毒等。

“震网”病毒是一种首次发现于 2010 年的恶性蠕虫电脑病毒，攻击的目标是工业上使用的可编程逻辑控制器（PLC）。作为一种网络战武器，“震网”（Stuxnet）病毒曾被用于实战，伊朗纳坦兹核设施就曾遭到过该病毒的侵袭。“震网”在侵入伊朗核设施的工业控制系统后，改变了离心机的发动机转速，这种转速的改变足以令离心机的运行能力受损并导致离心机的不可逆损坏。在震网病毒的肆虐下，伊朗纳坦兹的核工厂里可用的离心机数量从 4700 台降低到 3000 多台。到 2010 年，核工厂仍然因为技术问题多次停工，工厂的浓缩铀分离能力比去年下降了 30%。在离心机的功能被破坏后，“震网”还可向控制中心发送设备运行正常的反馈报告，从而达到悄然无声进行破坏的目的。

图 10：美军“震网”病毒袭击伊朗核设施过程



资料来源：公开网络、东兴证券研究所

图 11：伊朗纳坦兹的核工厂

资料来源：公开网络、东兴证券研究所

图 12：伊朗浓缩铀工厂的离心机

资料来源：公开网络、东兴证券研究所

袭击伊朗核设施的“震网”病毒具有三个显著特征：1. 具有很强的针对性，专门攻击工业控制系统，例如钢铁、汽车、电力、运输、水利、化工、石油等核心工业领域；2. 代价昂贵，使用了多个零日漏洞（零日漏洞指的是零时差攻击，是指被发现后立即被恶意利用的安全漏洞。通俗地讲，即安全补丁与瑕疵曝光的同一日内，相关的恶意程序就出现。这种攻击往往具有很大的突发性与破坏性。）；3. 定向性，具有明确的攻击目标，一次攻击专门针对一套系统。基于以上三个显著特征，我们可以对军用网络武器的破坏性有一个初步了解

“Fanny”蠕虫病毒可以对具备网闸隔离的网络进行攻击和侵入。这一蠕虫采用了基于通用串行总线（Universal Serial Bus，USB）的特殊控制机制，可通过优盘的感染与连接来进行侵入。当被感染 Fanny 蠕虫病毒的优盘被插入计算机后，该优盘中有一个极为隐秘的存储空间可用来对隔离网络的信息进行收集。被侵入的计算机在网络连接状态下，Fanny 蠕虫病毒可将收集到的相关信息实时传输给攻击者。若攻击者除了刺探相关情报信息外，还需要对被隔离的网络进行指令运行时，可通过 Fanny 蠕虫病毒事先将指令存储于优盘的隐匿空间中。当该优盘被连入计算机后，Fanny 蠕虫病毒会自动进行指令的运行。

“Regin”是一种极为高端的恶意软件，采用了诸多隐形技术，可以规避市面上常规的杀毒和安全软件检测。据全球知名信息安全企业赛门铁克（Symantec）公司的一项报告显示，“Regin”隐形间谍软件需要投入大量的资金和时间进行研发，这也表明该工具的身份并不普通。赛门铁克（Symantec）公司同时也指出，“Regin”隐形间谍软件被用于对政府、公司和民众进行监视。

“硬盘固件”病毒是 NSA 网络武器库有一种极为独特的网络战武器，该病毒事先就已被植入在硬盘固件中，用以对计算机进行感染。简言之，新买的计算机硬盘中，可能就已带有病毒。由于该病毒已被事先植入在硬盘固件中，因而即使是在未连接互联网的情形下，只需在硬盘通电后，这一病毒就会被激活。处于激活状态下的“硬盘固件”病毒，会在固件中建立一个隐匿的信息存储空间。不仅普通的硬盘分区和格式化对其毫无作用，即便是军工级别的磁盘擦除，都难以对其造成实质性清除。因此，计算机硬盘在被格式化，或者电脑操作系统被重装后，“硬盘固件”病毒仍可继续从被感染计算机处窃取相应数据信息。

2. 我国网军建设尚有不足

此次军改从部门、机关设置上搭建起了我国网军的主要骨架，但在网络靶场以及网络武器库建设方面尚属于初期阶段，还有巨大的发展潜力和市场空间。

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。

我国在网络靶场和武器库的建设目前也处于起步阶段，仅有部分科研实验室和行业专用试验场等，其主要功能是研究电子信息对抗与仿真技术、为行业产品进行试验及检测等。从体系应用角度来讲，我国现有的网络试验环境或测试床规模还较小，且主要针对某一专业领域，尚不适用于体系化的网络空间安全科研试验与测试评估。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，我国与美国都还存在着不小的差距。

3. 卫士通——助力网军建设关键所在

网络战若是新型核武器的话，那么卫士通可以说是网络安全领域的反导系统。其中卫士通在网络安全领域的防御能力我们在之前的报告中已经充分论证，本次我们将重点在网络靶场和网络攻防武器库的建设方面加以论证。

3.1 网络靶场和网络攻防武器库建设的复杂性

在 1.4.1 中我们分析了美国网络靶场建设的基本情况，那个可以从中得到几点启示作为我国国家级网络靶场的建设原则。

1. 国家级网络靶场的建设是维护国家网络空间安全的关键所在，是国家行为，体现国家意志、统筹国家资源、彰显国家能力。我国作为大国、网络大国和军事大国，应当具有与自身实力和地位相匹配的国家级网络靶场。

2. 国家级网络靶场是国家重要的战略资源，在建设国家网络靶场时，必须要对靶场有着清晰明确的定位和目标以及用户范围，完善的顶层设计，更需要集中网络高精尖力量，加快核心技术突破，走在网络技术前沿，这样才能使得网络靶场真正发挥作用。

3. 国家级网络靶场应紧密围绕建立先进的网络安全保障手段和高水平的综合性安全试验验证环境，服务于党政军重要信息系统，保障国家的关键基础设施安全，构建国家网络安全防护长城。

而在网络靶场功能需求方面，国家级靶场的功能应该主要满足以下功能需求:

1. 网络空间复杂性安全试验环境需求。进行网络空间复杂性安全试验需要国家网络靶场具备四方面的能力: 一是大规模复杂异构网络的快速复现能力，可以复现金融系统、工业控制系统、电信网和物联网等各类复杂异构网络; 二是复杂用户行为及网络舆情复现能力， 可以逼真模拟社会网络中人的行为和舆情行为; 三是网络空间复杂特征的复现能力，可复现网络空间融合性、隐蔽性、复杂性、无界性、高速性和层次性等复杂特征; 四是大规模网络快速灵活重组能力， 可从一个试验网络结构快速灵活重组成另一个试验网络结构。

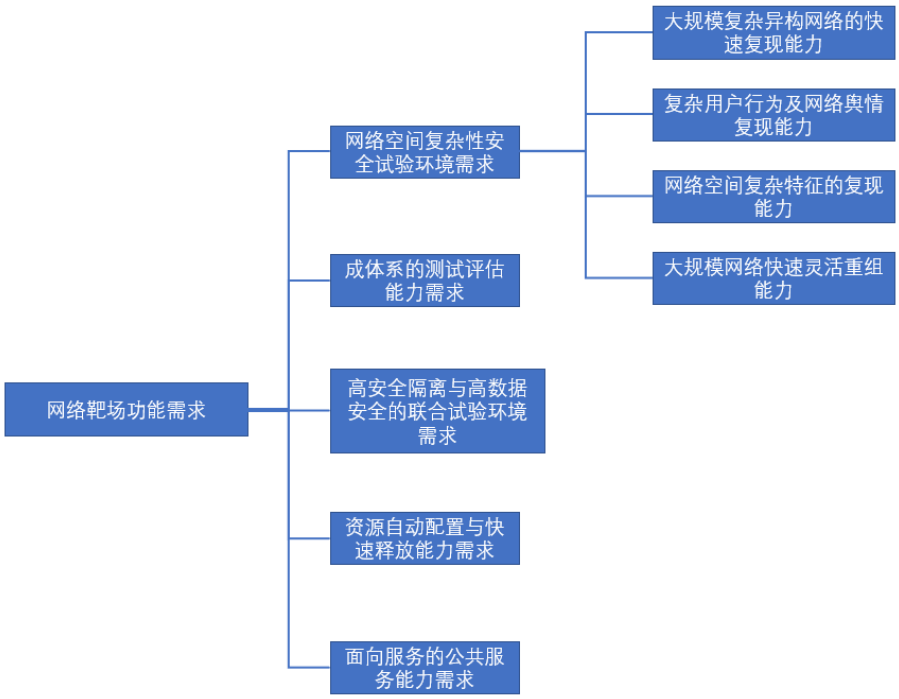
2. 成体系的测试评估能力需求。为了精确测试评估目标系统网络空间安全性、可恢复性和灵活性，操作系统、网络协议、内核等关键软硬件的安全性，国家网络靶场需具备成体系的测试评估能力。通过国家级完备的测试评估资源库（测试工具库、测试用例库等）及先进的测试评估手段，开展渗透测试、风险评估，对目标系统安全性进行全方位、体系化、自动化测试评估。

3. 高安全隔离与高数据安全的联合试验环境需求。为了并行开展不同安全等级网络的试验而不影响各试验网络与数据安全，需要构建高安全隔离与高数据安全的联合试验环境。在联合试验环境中可并行开展多个不同安全等级的安全技术测试、各种恶意软件和恶意代码测试等试验，而不用担心试验基础设施安全。并行试验之间不会相互干扰，重要数据也不会在试验中泄漏。

4. 资源自动配置与快速释放能力需求。为了实现国家网络靶场内部各类异构共用资源（网络、计算、存储、信息等）的集中管控和灵活调用，使其利用率最大化并保证用户对资源使用的有效性，需具备资源自动配置与快速释放能力。

5. 面向服务的公共服务能力需求。为了实现不同网络空间安全试验资源的即插即用、动态共享、重用和互操作，国家网络靶场需具备面向服务的公共服务能力，建立服务化、智能化、网络化、模块化的网络共用基础设施集成环境，为各功能系统面向服务的部署、集成、运行与管控提供全过程支撑。

图 13：靶场功能需求分析



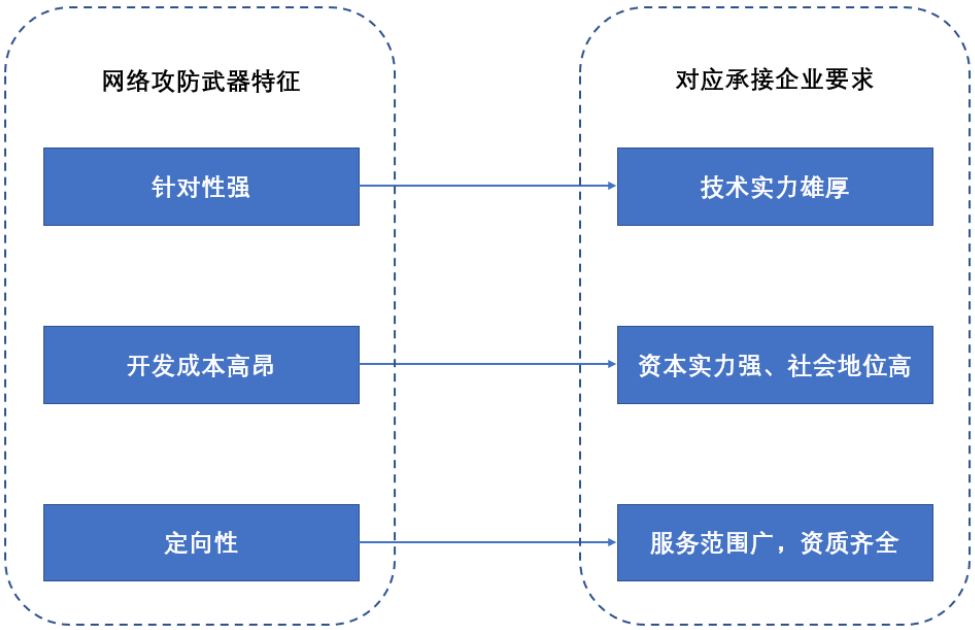
资料来源：《国家网络靶场的建设与发展》、东兴证券研究所

而具体建设方面，我们参考 1.4.1 中内容，可以归纳为：1. 重点网络靶场的建设多由国家级安全部门牵头；2. 网络靶场一般有多个层级，最上层级为国家级的联合网络靶场，适用范围大，内容涵盖广，用户种类多。而次级靶场如军用或某些工业领域专用靶场在特定内容和适用领域有所突出，强调专业性；3. 网络靶场的建设、运营和维护多采取出军民融合的模式，大部分都交给网络安防领域实力强大的军工或专业软件企业负责。

其中第三点中是关于网络靶场的建设以及后续的运营维护的主要负责单位应为我国网络安全领域的领军企业或单位。

而我们在“震网”病毒中了解到这种原本在美国网络武器库中的杀器具有针对性强，成本高昂和定向性的特点，也就意味着网络武器库的建设并非普通的网络安全企业所能承担，只有能够对应满足上述特征的单位具备承接网络武器库的建设。其中仅资质问题一项就已经将能够承担项目的企业单位范围压缩至很小。

图 14：网络攻防武器库建设要求



资料来源：东兴证券研究所

普通的网络安全企业无法满足网络靶场和攻防武器库的建设要求，其中仅资质问题一项就已经将能够承担项目的企业单位范围压缩至很小。

图 15：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

即便在国外也只有洛克希德·马丁、BAE 系统公司、诺斯罗普·格鲁曼等少数军工巨头能够承接政府和军方的建设项目。

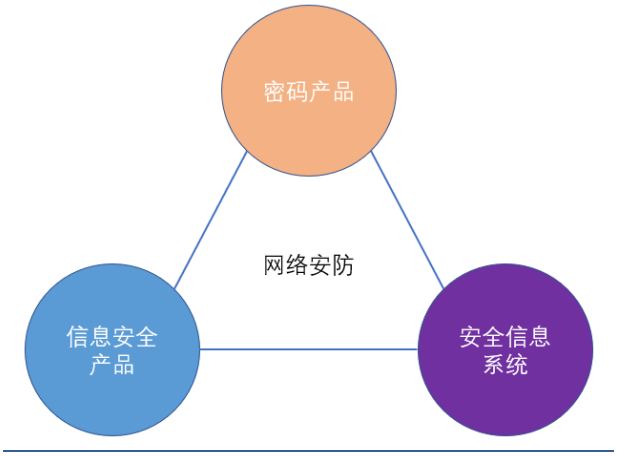
3.2 卫士通完美符合网军基础设施建设的要求

回看我国，中国电子科技集团下属中国网安公司是根据国家安全战略发展需要，以深耕信息安全 和物理安全领域的中国电科三十所、三十三所为核心，汇聚中国电科内部资源重点打造的网络信息安全子集团，中国网安凭借在密码保密、信息安全和物理安全领域的深厚积淀，奠定了坚实雄厚的行业地位，在国家信息安全核心和重要领域占据绝对领先的市场份额,打造了 包括中国信息安全第一股“卫士通”在内的多家信息安全公司。作为我国网络安全领域的中坚力量，不论从身份地位还是技术实力看都是我国网络靶场和网络攻防武器库的主要建设单位的不二之选。

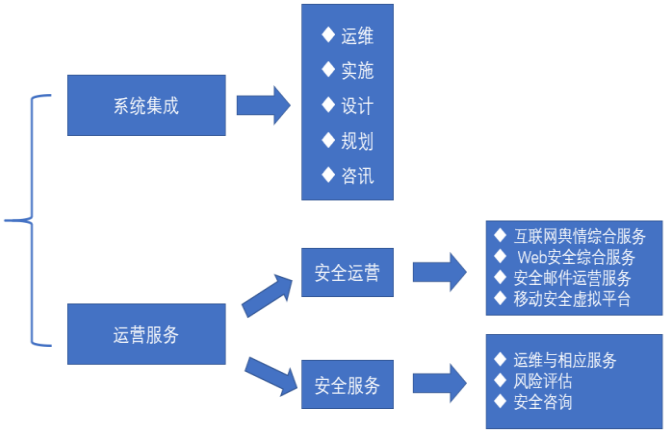
卫士通公司深耕网络安全领域多年，拥有国内顶级的信息安全资质，最强的信息安全研发团队，最完善的质量服务体系，网络安全理念、技术和产品均为国内顶尖；卫士通产品谱系齐全，应用广泛，满足服务范围广的要求；同时作为上市公司，卫士通具有拥有良好的资本平台，能够承受成本高昂的研发费用。

图 16：卫士通产品范围均围绕网络安防

图 17：卫士通服务与支持紧扣网络安防



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

此外卫士通积累了大量的客户资源，其中包含数量众多的定制服务与产品，产品和服务具有针对性和专业性，这就意味着卫士通在诸多领域具有相关的专业经验，能够有效将网络安防内置于相关行业领域，而非一本通似的草草解决问题。因此卫士通在建设多功能、多服务对象的网络靶场和攻防武器库上具有极大的优势。

表 5：卫士通产品和客户范围

产品/系统解决方案	行业解决方案/客户种类
网站安全防护解决方案	政府
安全隔离与信息交换	央企
综合安全监管解决方案	公检法
安全桌面云解决方案	金融
云监管平台解决方案	能源
	其他

资料来源：公司官网，东兴证券研究所

大股东中国网安公司和中国电子科技集团是公司的坚实后盾，根据市场需求，进一步深化军民融合、军工资产注入等要素逐步到位，卫士通有能力对大数据、云计算、移动互联网和物联网领域进行全面覆盖。

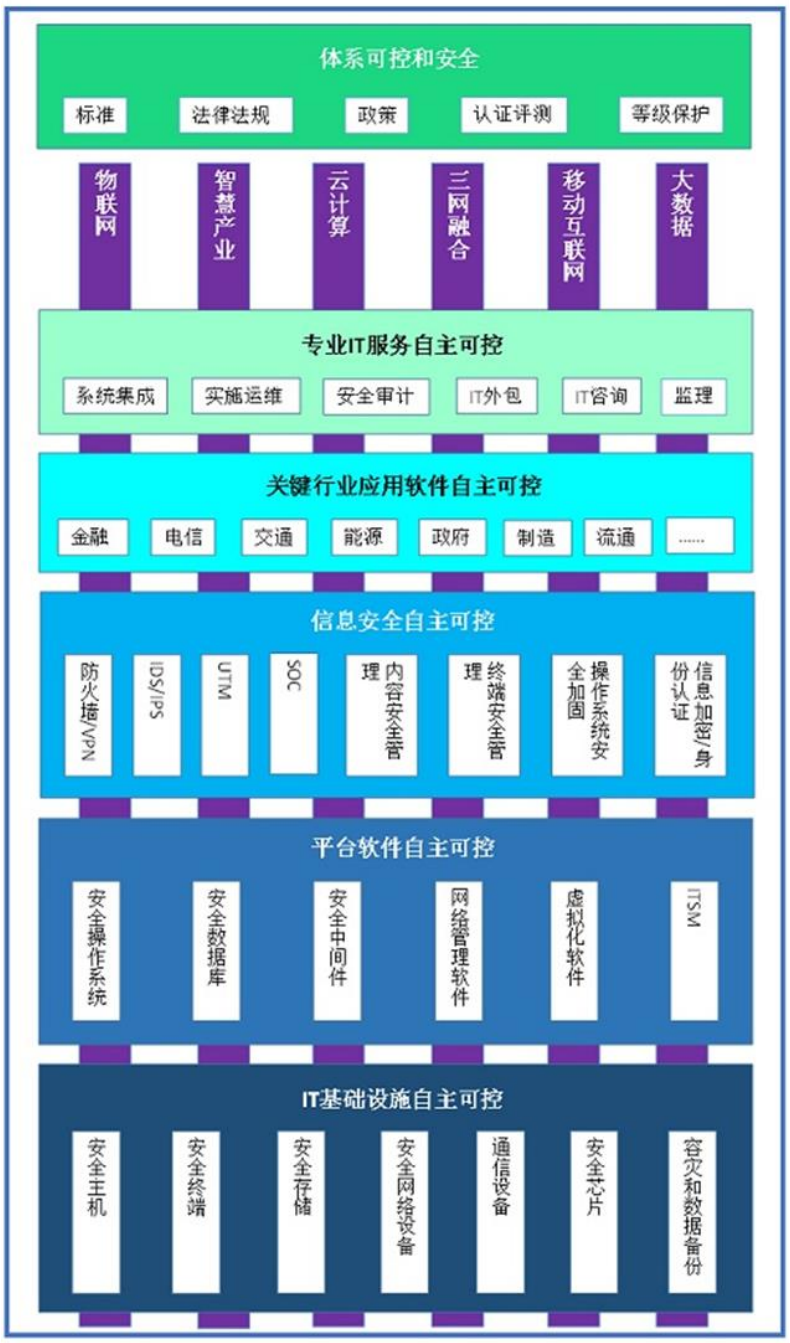
3.3 自主可控——网军建设和网络真正安全的必要条件

自主可控是保障网络安全、信息安全的必要条件。能自主可控意味着信息安全容易治理、产品和服务一般不存在恶意后门并可以不断改进或修补漏洞；反之，不能自主可控就意味着具“他控性”，就会受制于人，其后果是：信息安全难以治理、产品和服务一般存在恶意后门并难以不断改进或修补漏洞，同时中兴事件也充分说明了坚持关键信息技术安全可控是保证我国经济发展、社会稳定和国防安全的重要环节，是打破现有技术封锁、实现核心技术不受制于人的必要条件。

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”。

目前我国行业整体存在自主可控问题，许多行业的核心技术和设备来源均为海外。自主可控全景图分为体系可控与安全、专业 IT 服务自主可控、关键行业应用软件自主可控、信息安全自主可控、平台软件自主可控、IT 基础设施自主可控等六部分。

图 18：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

那么自主可控在网络安全、网络战争和网军建设领域的重要究竟几何，我们再来回顾前文介绍的“震网”病毒攻击伊朗核设施导致伊朗核计划受阻事件，重点关注几个细节：

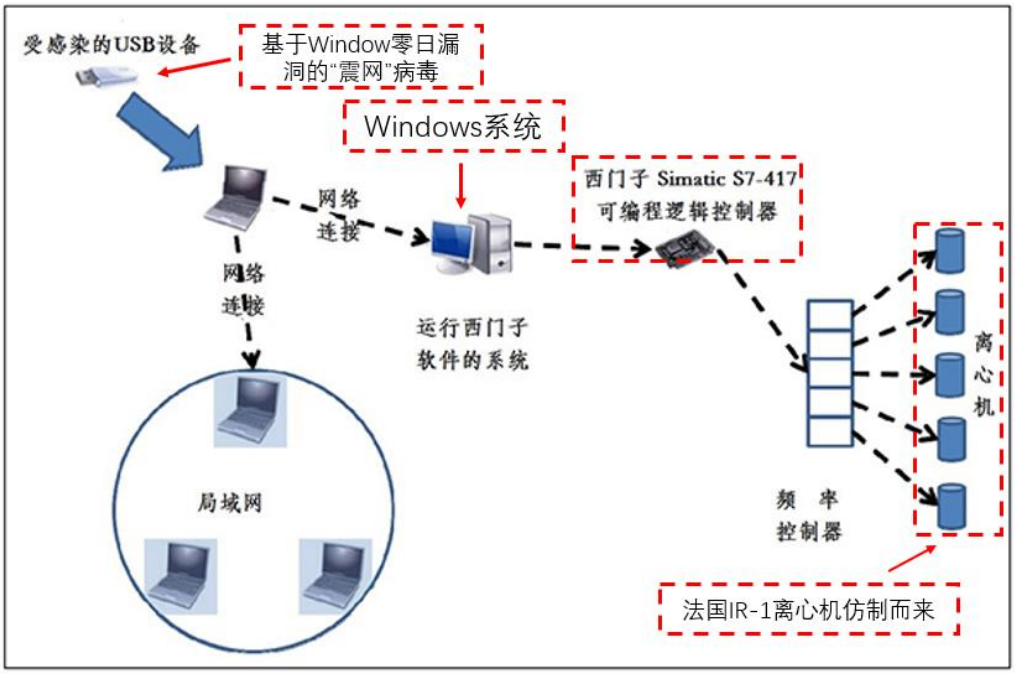
1. 伊朗核设施的操作系统使用的是 **Windows** 系统。

2. “震网”病毒威力巨大很大原因在于使用了多个 **Windows** 零日漏洞。

3. 伊朗核设施使用的离心机是从上世纪 60 年代经巴基斯坦走私而来的**法国制造 IR-1 离心机**，必须使用特定的 Safe 系统。

4. 伊朗核设施所用的离心机使用的是西门子 **Simatic S7-417 可编程逻辑器件**。

图 19：伊朗核设施自主可控隐患



资料来源：东兴证券研究所

可以发现，伊朗核设施在关键领域均使用了国外的技术和设备，这是“震网”病毒能够成功破坏核设施的关键所在。因此是否实现自主可控，是网军能否发展壮大以及网络战争能否取胜的关键所在。

2016 年 3 月 4 日，我国安全可靠技术和产业联盟成立。

联盟的业务工作范围是：一、开展我国安全可靠技术发展领域的战略及策略研究，支撑形成安全可靠软硬件发展的顶层设计；二、开展安全可靠关键技术、标准制定、发展路线等相关研究；三、组织开展安全可靠领域的人才培育、认证等相关工作；四、组织建立安全可靠领域的联合实验室，开展技术、产品、方案和安全等方面的技术研究工作，推进产品适配验证，系统优化改进；五、组织协调安全可靠领域的产学研用共同营造健康的安全可靠生态环境。

安全厂商（6 家）包括：星网锐捷（通信、安全）、中孚信息（安全保密）、安宁创新（邮件、消息）、中安网脉（密码、存储）、海泰方圆（密码、安全）、卫士通（密码、芯片、系统）。

卫士通作为联盟成员，重点布局安全领域，并与其它自主可控公司一起打造全产业链自主可控生态体系。

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。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。

因此可见，卫士通作为国内网络安全领域自主可控的领军企业，有望在网军建设中发挥出重要作用。

4. 投资建议

站在当前的时点，我们仍然坚定看好，公司 2019 年几大新业务进入收获期，我们预测公司 2019 年~2020 年利润分别为 5.47 亿、8.07 亿，EPS 分别为 0.65 元、0.96 元，维持“强烈推荐”评级。

5. 风险提示

网军建设进度低于预期。

表 6：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	4311	9773	14334	**营业收入**	1799	2137	1931	5227	7692
货币资金	524	1881	2315	4600	6769	**营业成本**	1165	1383	1234	3054	4393
应收账款	1088	1616	1460	3953	5817	营业税金及附加	15	20	6	17	25
其他应收款	59	67	60	163	240	营业费用	177	215	203	549	808
预付款项	55	68	80	109	151	管理费用	271	330	319	810	1192
存货	193	211	188	466	670	财务费用	6	-12	-21	69	233
其他流动资产	29	25	27	-5	-29	资产减值损失	47.47	74.60	63.63	76.62	71.31
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	129	653	972
无形资产	10	71	63	57	51	营业外收入	76.69	50.75	23.86	41.92	48.92
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	5775	11073	15472	**利润总额**	196	203	152	694	1020
流动负债合计	2026	1309	1234	6146	9978	所得税	23	26	12	139	204
短期借款	829	0	0	3465	6198	**净利润**	173	177	140	556	816
应付账款	759	980	863	2136	3072	少数股东损益	17	8	0	8	8
预收款项	40	60	77	124	193	归属母公司净利润	156	169	140	547	808
一年内到期的非	0	0	0	0	0	EBITDA	161	238	272	886	1368
非流动负债合计	50	57	57	57	57	**EPS（元）**	0.36	0.21	0.17	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	1291	6202	10035	**成长能力**					
少数股东权益	84	92	92	100	108	营业收入增长					
实收资本（或股	433	838	838	838	838	营业利润增长	12.21%	18.80%	-9.64%	170.68%	47.16%
资本公积	300	2558	2558	2558	2558	归属于母公司净利润	-9.33%	28.11%	-15.98%	407.71%	48.79%
未分配利润	708	848	902	1113	1424	**获利能力**	4.69%	8.54%	-17.22%	291.08%	47.61%
归属母公司股东	1489	4296	4392	4770	5328	毛利率(%)					
负债和所有者权	3649	5754	5775	11073	15472	净利率(%)	36.10%	41.58%	42.89%	42.30%	43.14%
现金流量表				单位:百万元		总资产净利润（%）		9.61%	8.29%	7.25%	10.63%
	2016A	2017A	2018E	2019E	2020E	ROE(%)	4.27%	2.94%	2.42%	4.94%	5.22%
经营活动现金流	-137	-51	460	-866	-12	**偿债能力**	10.46%	3.94%	3.19%	11.47%	15.16%
净利润	173	177	140	556	816	资产负债率(%)					
折旧摊销	35.55	97.30	0.00	157.02	157.02	流动比率	57%	24%	22%	56%	65%
财务费用	6	-12	-21	69	233	速动比率	1.06	3.11	3.49	1.59	1.44
应收账款减少	0	0	156	-2492	-1864	**营运能力**	0.96	2.95	3.34	1.51	1.37
预收帐款增加	0	0	17	47	69	总资产周转率					
投资活动现金流	-634	-181	-4	-75	-70	应收账款周转率	0.57	0.45	0.33	0.62	0.58
公允价值变动收	0	0	0	0	0	应付账款周转率	2	2	1	2	2
长期股权投资减	0	0	0	0	0	**每股指标（元）**	2.59	2.46	2.10	3.49	2.95
投资收益	2	2	2	2	2	每股收益(最新摊薄)					
筹资活动现金流	733	1579	-22	3226	2250	每股净现金流(最新	0.36	0.21	0.17	0.65	0.96
应付债券增加	0	0	0	0	0	每股净资产(最新摊	-0.09	1.61	0.52	2.73	2.59
长期借款增加	0	0	0	0	0	**估值比率**	3.44	5.12	5.24	5.69	6.36
普通股增加	0	406	0	0	0	P/E					
资本公积增加	6	2258	0	0	0	P/B	76.23	130.16	164.43	42.05	28.49
现金净增加额	-38	1347	434	2285	2169	EV/EBITDA	7.97	5.36	5.24	4.82	4.32

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。