

科技战本质是网络战，网安携“乌媒”布局互联网监管

——“安全可靠工程半月谈”第二期

投资摘要：

1、当前中美科技战本质是网络战。科技战的背后是网络战，以及对网络数据的争夺。美国的国家级网络部队正试图通过开展科技战打压华为，获取 5G 时代对网络数据的截获和监听。当今网络时代的对手不仅是病毒、木马、诈骗短信，更多的是其他国家的网络战部队。网络战的表现形式也不仅限于 DDOS 攻击，而是潜伏在对手网络中数年，等待时机将网络攻击至瘫痪。未来，网络战的重要职责之一是情报战，即国家情报机构和网络战部队通过网络攻击方式入侵电脑获取文档，对另一个国家发起的渗透和情报窃取。在物联网时代，网络攻击伤害将更大。由于每一个设备都有小的操作系统，都可能存在漏洞，进而成为被攻击的一个要点。而物联网的攻击力度、防守难度将比电脑发起的攻击增加很多倍，所有网络虚拟空间的攻击都可以变成物理世界的伤害，例如电站断电、高铁停运、发布不实消息等。

2、中国不会步日本后尘，5G 和 AI 将是保持我国高速增长的利器。与当时日本半导体处境类似，我国 5G 产业被打压也是借着美国国家安全的理由。但不同的是，中国有一个庞大的内需市场。美国想通过极限施压的封锁策略击垮华为和中国的半导体芯片行业，无疑将对其自身的芯片和软件业带来歼灭战式的打击。依托庞大的国内市场和完整的产业链布局，叠加政府政策支持和成立集成电路大基金的资金支持，中国半导体行业有望抗住这次中美科技战的冲击。与日美芯片战不同的是，日本签订《美日半导体协议》后日本是被迫打开国内 20% 以上的市场份额，而此次中美科技战在国内庞大市场和完整产业链布局情况下，我国半导体产业有望凭借接管美国禁运后的对芯片产品的需求缺口，而不是步日本后尘。我们应当清醒的是，5G 和 AI 是保持我国工业和服务业提升效率的必由之路，上游的一些阻碍可以借助本土芯片厂商崛起而得到解决，不能阻止中国在 5G 和 AI 方面的进步。

3、互联网监管体系重构升级，网安携“乌媒”布局互联网监管。随着互联网飞速发展，互联网对于生产资源的重新分配、生产方式改革都迫切要求立法和监管部门做出全面回应。中国网安针对互联网监管方面的需求，多点布局多媒体信息安全。二零凯天是中国网安旗下专注于多媒体通信与信息安全技术的核心成员企业，以多媒体通信、智能图像处理与分析、多媒体信息安全为核心技术，定向专研“信息安全”与“人工智能”相关技术研发，推出了以安防摄像头为核心的“二零视盾”一体化安全保密安防系统。同时二零凯天针对社会对网络空间的良好生态需求，打造了“乌媒”新媒体内容监测平台，通过对指定视听网站、微信公众号等自媒体平台的内容（图片、视频）进行主动爬取和内容识别，将识别到的受控视图、色情低俗、暴恐等不良内容通过页面方式进行展示。产品已有效应用于多个省区市网信与公安部门，并取得良好的社会效益。

2019 年 05 月 27 日

看好/维持

国防军工 周期报告

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

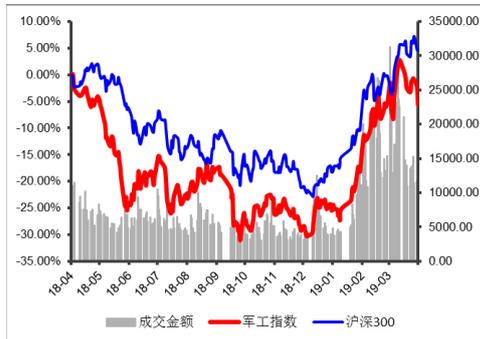
研究助理：张卓琦

010-66554018 Zhangzq_yjs@dxzq.net.cn

执业证书编号：S1480117080010

细分行业	评级	动态
密码行业	看好	维持
行业基本资料		
		占比%
股票家数	53	1.46%
重点公司家数	3	
行业市值	8325.13 亿元	1.32%
流通市值	544.01 亿元	1.09%
行业平均市盈率	89.51	/
市场平均市盈率	16.54	/

行业指数走势图



资料来源：东兴证券研究所

相关研究报告

1、《安全可靠工程半月谈第一期：等保 2.0 出台在即 网安央企大力度混改》2019-05-13

投资建议：在网络战范畴下，互联网监管和芯片自主可控都是我国的必然选择方向，建议重点关注互联网监管国家队卫士通和国产 CPU 龙头中国长城。

行业重点公司盈利预测

简称	EPS (元)			PE			PB	评级
	18A	19E	20E	18A	19E	20E		
卫士通	0.19	0.65	0.96	156	45	31	5.63	强烈推荐
中国长城	0.34	0.44	0.56	27	21	16	4.35	强烈推荐

目录

1. 互联网监管体系重构升级，网安的新产品布局内容安全监管	5
1.1 我国互联网监管法规政策变迁	5
1.2 网安布局多媒体信息安全，推出“乌媒”内容安全监测	6
1.2 “乌媒”不良内容监管平台实战案例	12
2. 中美科技战实则为网络战	12
2.1 中美科技战序幕拉开，同时吹响网络战的号角	12
2.2 日美芯片战“上下半场”的前车之鉴	15
2.3 中国内需市场庞大，制造业独具优势	18
3. 科技赋能服务业，本土供应商崛起，是我国保持经济高增速的必然需求	19
3.1 改革开放、科技创新提升服务业效率，迎接经济高收入阶段关键挑战	19
3.2 华为：为本土供应商带来巨大自主可控机会	24
4. 风险提示	27

表格目录

表 1：美国网络空间国防发展轨迹	13
表 2：各国网络战抓总机构成立时间表	14
表 3：各国网络作战部队组建时间表	14
表 4：华为 25 家大陆供应商盘点	25
表 5：华为的 33 家美国供应商	25
表 6：重点跟踪公司	28

插图目录

图 1：“三零视盾”一体化安全保密安防系统	7
图 2：三零视盾综合安防管理平台	7
图 3：乌媒不良媒体内容监管平台	8
图 4：“乌媒”新媒体内容监测平台系统架构	9
图 5：引擎产品示意图	9
图 6：网络大数据分析系统示意图	10
图 7：乌媒不良媒体内容监管平台	11
图 8：美国国防及网信领域动员组织体系	13
图 9：1975-2010 年全球半导体市场份额变动图	17

1. 互联网监管体系重构升级，网安的新产品布局内容安全监管

1.1 我国互联网监管法规政策变迁

我国互联网监管肇因于发展需求和安全需求之间的政策价值矛盾。中国社会所处的发展阶段和在国际政治中的特殊地位要求政府必须通过行之有效的行政监管，在尽可能发挥互联网对于促进经济增长，改革创新等积极作用的同时，将其对社会稳定、国家安全的负面影响控制到最低。中国互联网监管历史阶段划分如下：

第一阶段：监管的引入与奠基（1994~1999）

《计算机信息系统安全保护条例》（国务院令 147 号）是我国第一部涉及互联网管理的行政法规。此后三年间，我国集中针对国际联网出台了若干法规政策，开创了我国互联网监管的奠基性制度，其中很多规定沿用至今，在实践中发挥重要作用。例如：国际出入口信道专营制度；联网接入的许可、备案制度；计算机系统等级保护制度等。这些管理制度保证了国际联网的可管可控，通过对管道的监管，实现内容监管目标。

第二阶段：监管体系全面建立阶段（2000~2007）

步入 2000 年，以《互联网信息服务管理办法》（国务院第 292 号令）为标志，中国互联网监管进入了体系化阶段。《互联网信息服务管理办法》是我国互联网监管的基础性法规，它的出台标志着监管从早期的渠道层向应用层深化。作为重要的上位法，它为各部委开展部门规章立法，确立更为详细的监管规范提供了法律依据。各部门据此建章立制，完成监管边界的“跑马圈地”，监管部门之间的合作与竞争并存。

依据法规规章，我国全面建立互联网内容监管制度：

- 对新闻、出版、教育等互联网信息服务实行前后置审批的双重许可制度（即有关管理部门的前置审批加电信管理部门的许可或备案）；
- 明确规定“九不准”；
- 建立了完善的互联网内容监管机制，包括：合法经营主体公示制度，上网信息记录制度，违法信息保存与报告制度，协同配合制度。全面引入了事前（以许可为主），事中（以企业监测为主），事后（以关闭网站、吊销许可为主）的全流程管理手段。

第三阶段：监管优化与扩展阶段（2008~2012）

这一时期的立法与制度建设鲜明体现了“优化扩展”特点。2010 年 9 月，《互联网信息服务管理办法》修订工作启动，以通过立法确认新的监管体制，并以此为契机，对互联网监管制度做出进一步完善。部分部委也陆续启动对互联网监管规章的修订工作。

除“优化”外，这一阶段的监管工作不断扩展。区别于过去以内容监管核心，本阶段更多的引入了经济、市场类监管主体和监管机制，监管议题不断丰富。例如：

- 不正当竞争监管。伴随产业发展壮大，互联网市场竞争愈加激烈，并最终演化为具有历史标杆意义的“3Q 大战”，促使行业主管部门紧急出台《规范互联网信息服务市场秩序若干规定》，首次对互联网竞争树立行为边界。

- 电子商务、网络支付、网络税收等经济监管议题浮现。工商总局、央行、国家税务总局分别出台相应规章、规范性文件，建立初步监管框架。
- 个人信息保护问题受到关注。以 2012 年全国人大关于加强网络信息保护的决定为依据，工信部出台互联网领域的个人信息保护规章，探索个人信息保护行政监管机制。

第四阶段：监管重构升级阶段（2013~现在）

2013 年开始，产业互联网全面爆发，互联网对于生产资源的重新分配、生产方式改革都迫切要求立法做出全面回应。互联网立法层级更高，适用领域更宽，调整程度更深。《反恐怖主义法》、《国家安全法》、《网络安全法》、《食品安全法》、《广告法》、《电子商务法》等一批国家大法陆续出台或优先列入立法议程。其中无论是专门新立的网络法，还是过去传统法律修订，围绕网络的法律制度构建无疑都成为立法核心，覆盖网络安全、产业发展、平台责任、业务监管，议题愈加宏大和深入。

安全类监管与市场类监管的制度区隔愈来愈明显，前者趋紧和加深，从网络层到数据层全面建立安全屏障，建立关键基础设施保护体系、网络安全审查制度，跨境数据流动评估制度等等；后者呈现宽容和放松心态，针对网络约车、互联网金融等新兴业态，在保障消费者利益、维护市场秩序基础上，对数字经济的新模式予以合法地位。

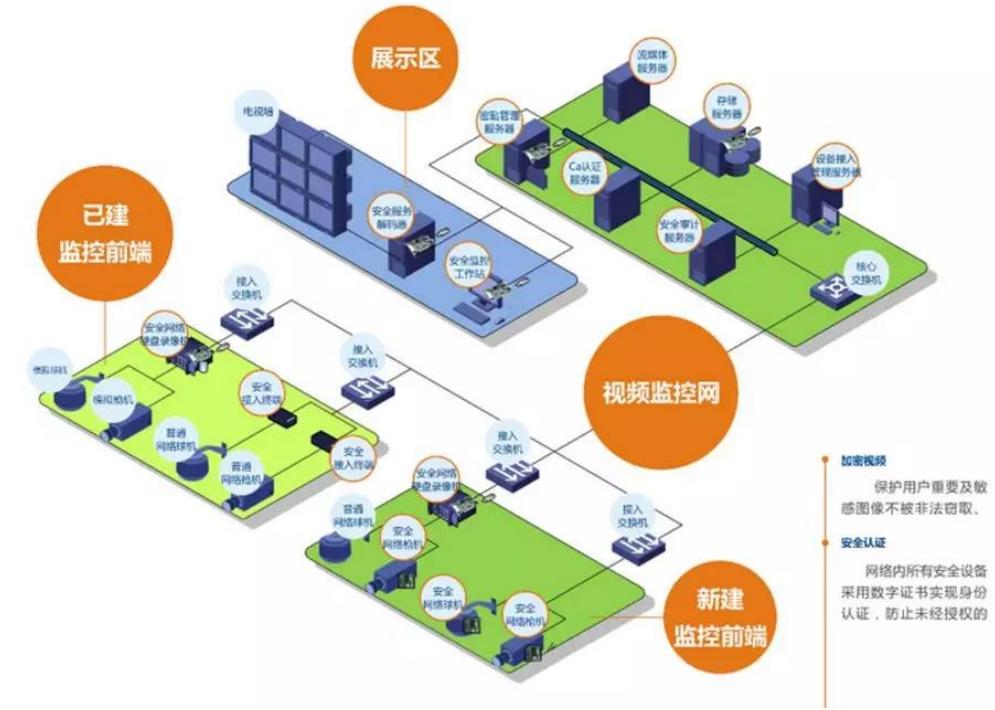
1.2 网安布局多媒体信息安全，推出“乌媒”内容安全监测

二零凯天是中国网安旗下专注于多媒体通信与信息安全技术的核心成员企业，以多媒体通信、智能图像处理与分析、多媒体信息安全为核心技术，公司成立于 2001 年。经过多年的发展，逐步确立了媒体安全、安全监控和安全运营三大业务方向，公司以图像识别及密码应用为核心，定向专研“信息安全”与“人工智能”相关技术研发，着力打造具有信息安全及智能识别特性的产品与系统解决方案，解决行业用户需求。

“二零视盾”一体化安全保密安防系统：是二零凯天依托中国网安在密码及信息安全方面强大的科研技术实力，自主开发的、具有知识产权的综合安防管理系统。

系统形成了覆盖前端设备到后端管理平台的完整产品解决方案，可实现数据采集、传输、存储和应用过程中的安全防护。系统有效解决摄像机被人为更换；传输过程中数据被篡改、完整性被破坏；存储过程中出现的数据篡改、泄露；中心应用过程中出现访问控制等方面的安全问题。

图 1：“三零视盾”一体化安全保密安防系统



资料来源：公司官网，东兴证券研究所

“三零视盾”安防系统构建的智能管理系统平台，融合访客，门禁，车辆，监控，报警，资产管理等安防子系统数据，实现各子系统数据实时关联分析，将分析结果进行多维态势呈现，给用户最想要的结果和细节呈现。

图 2：三零视盾综合安防管理平台



资料来源：公司官网，东兴证券研究所

伴随着新媒体的业务创新，新媒体内容及监测业务变得多样化，新媒体环境给内容监管带来新的挑战：新媒体播出内容海量，如何依靠有限的人员完成海量内容监管，是目前面临的新课题。

作为中国网安媒体安全领域的骨干力量，三零凯天公司针对社会对网络空间的良好生态需求，打造了“乌媒”新媒体内容监测平台。通过实现属地网站视听内容的监测监管，通过对指定视听网站、微信公众号等自媒体平台的内容（图片、视频）进行主动爬取和内容识别，将识别到的受控视图、色情低俗、暴恐等不良内容通过页面方式进行展示。产品已有效应用至多个省区市网信与公安部门，并取得良好的社会效益。该平台在网络空间治理过程中发挥了不可替代的傲人作用，为网信、公安、运营商、军队和广电等行业监管部门的内容监管、情报挖掘工作提供有效的技术手段，为社会发展营造更加清朗的网络空间。

- **监测内容：**暴恐内容识别、色情内容识别、政治有害内容识别、敏感视图像布控与识别、大规模视图像检索、涉藏涉疆元素识别。
- **监测范围：**属地网站监测、新闻、视频 APP 监测、微信公众号监测、微博监测、网络直播平台监管。
- **关键技术：**分布式网页数据采集技术、视频指纹技术、分布式存储技术、基于深度学习的视觉内容检测技术。

图 3：乌媒不良媒体内容监管平台

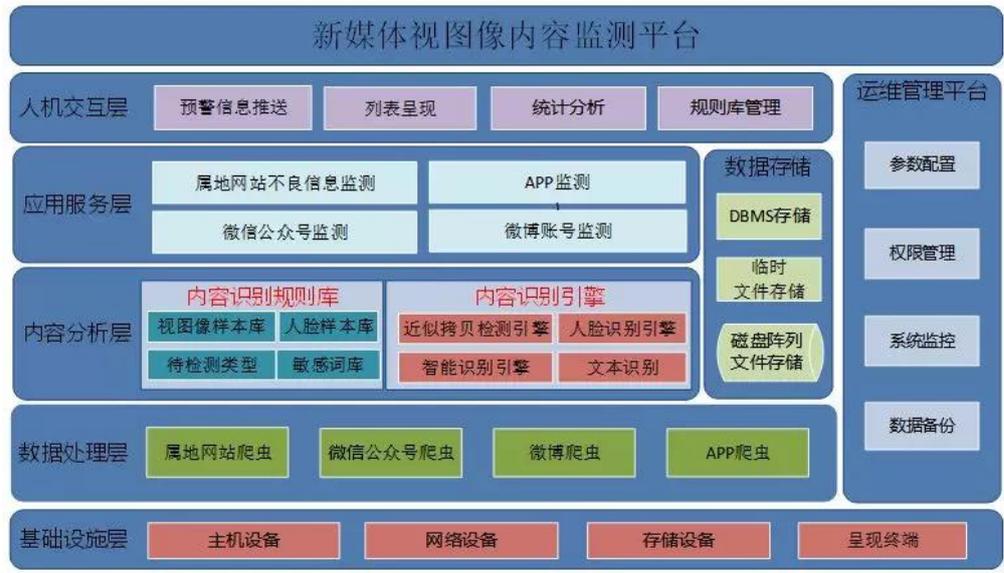


资料来源：公司官网，东兴证券研究所

“乌媒”家族包含引擎、工具、系统、平台，主要能够完成以下工作内容：

- 基于数据源调度方式的多通道分布式数据采集技术、
- 视图像近似拷贝检测技术、
- 基于深度学习的视图像内容分类技术
- 目标检测识别技术、
- 非规则背景下的 OCR 识别技术

图 4：“乌媒”新媒体内容监测平台系统架构

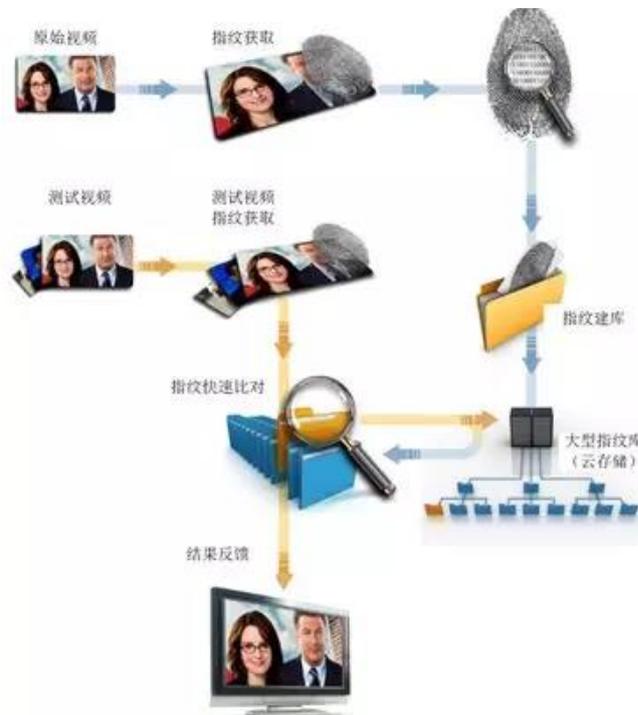


资料来源：公司官网，东兴证券研究所

(1) 引擎

乌媒的“引擎”可以将受控敏感视频采用“视频指纹技术”生成视频指纹库，将需要识别的媒体内容与视频指纹库进行快速匹配，判断目标视频是否为源视频，且不受各类形变及分辨率影响，应用于不良视频匹配，为重点网络空间场所的巡查提供图像、视频内容分析的技术手段，实现已知有害图片、视频在网络空间的反渗透。

图 5：引擎产品示意图



资料来源：公司官网，东兴证券研究所

“引擎”绝技：

- 支持对视频和图像的近似拷贝检测；抗干扰能力强，可有效识别翻拍、裁剪、片段拼接、画中画等多种形变；
- 单台超算服务器识别速率 ≥ 40 张/秒，识别准确率 $\geq 95\%$ 、召回率 $\geq 80\%$ 。

“引擎”优势：

已进行数亿条多媒体内容的检测、三十余次版本迭代，引擎具有很强的可复制性。

（2）工具

乌媒的比对“工具”可以基于深度学习的面部分析技术以及计算机视觉技术，通过人脸检测与分析、人脸比对与验证等，实现互联网视频中相对高质量人脸抓拍及画面快速定位。

“工具”绝技：

- 支持图片/视频中人脸检测分析、人脸比对、人脸检索等识别功能；
- 视频人脸的高效定位：毫秒级画面定位；单台超算服务器图片命中率 $\geq 95\%$ ，识别速率 ≥ 40 张/秒。

“工具”优势：

紧密贴近公安部门一线作战的实际需求，针对性强，性价比高。

（3）系统

乌媒的“系统”可以将对用户内容平台推送的图片、视频、敏感文档内容进行匹配及分析，快速甄别出海量信息中敏感内容，为其他子系统提供有效线索，以此对潜在 BK 隐患提供早期预警以及案件的情报分析。

图 6：网络大数据分析系统示意图



资料来源：公司官网，东兴证券研究所

“系统”绝技：

- 多模型识别能力；支持分析的文件类别：图像、视频、PDF 等敏感文档；
- 支持多种文件采集方式：DPI 爬虫、FTP、HTTP 等；
- 单台超算服务器特定场景或特定目标的识别准确率 $\geq 95\%$ 。

“系统”优势：

经过多地公安的实战演练和特殊数据支撑，产品在网络空间暴恐内容识别以及情报的早期发现方面具有很强的实战价值。

(4) 平台

乌媒的“平台”可以通过视觉计算、人工智能识别，对互联网敏感视图像内容进行分析及布控，实现“两微一端一站”以及直播平台的覆盖，实现对视频、图像、文字等内容的监测监管及情报挖掘。

图 7：乌媒不良媒体内容监管平台



资料来源：公司官网，东兴证券研究所

“平台”绝技：

- 多通道多来源数据采集；
- 内容识别分析；
- 丰富的监测列表、监测内容展示形式；
- 支持多层数据内容采集。

“平台”优势：

数据源接口丰富、识别范围广、视图像模型种类多。

1.2 “乌媒”不良内容监管平台实战案例

网信行业：“乌媒”系列引擎、平台类产品已经成功在中央网信办、贵州省网信办、南部县网信办形成销售，有效弥补了各级网信办在互联网视图像内容监管上的短板；为各级网信办在互联网空间的巡查、监管提供图像、视频内容识别、分析和预警技术手段，实现对已知有害图片、视频在互联网空间的反渗透能力，有效地配合网信部门完成了“国庆”、“春节”、“两会”等重大时期的技术保障工作。

公安行业：“乌媒”系列引擎、工具、平台类产品目前已经在上海、福建、广东等地的地市、区县级公安网监进行试用和应用，为公安作为网络信息安全监管部门落实《网络安全法》、《公安机关互联网安全监督检查规定（公安部 151 号令）》的内容监督检查工作提供技术手段。

首创“人工智能+多媒体情报挖掘”的技术查缉手段，联合某公安局围绕“智慧反恐”开展深度警企合作，系统类产品已投入实战。

运营商行业：“乌媒”系列平台类产品可及时发现、识别、封堵 IDC 流量中的色情、暴恐、政治有害、电信诈骗、赌博等不良内容，目前在贵州、四川省级移动公司 IDC 机房进行部署应用，为运营商对 IDC、CDN、专线、自有网站的文字、图片和视频不良信息的监管和处置提供技术手段，极大提高了运营商针对互联网内容治理监督检查工作的有效性、时效性和准确性。

广电传媒行业：“乌媒”系列平台类产品已经在绵阳广电进行应用，为广电对属地网站及两微一端的内容监管和治理提供了高效快捷的技术措施，形成了覆盖网络传媒中心新媒体视图像内容的统一审查平台，有效提高对网络传媒中心融媒体平台上违规、敏感、不良视图像内容的标准化审查，在行业具备较强的复制性。

2. 中美科技战实则为网络战

科技战的背后是网络战，以及对网络数据的争夺。美国的国家级网络部队正试图通过开展科技战打压华为，获取 5G 时代对网络数据的截获和监听。当今网络时代所应对的对手不仅是病毒、木马、诈骗短信，更多的是其他国家的网络战部队。网络战的表现形式也不仅限于 DDOS 攻击，而是潜伏在对手网络中数年，等待时机将网络攻击至瘫痪。

2.1 中美科技战序幕拉开，同时吹响网络战的号角

华为禁令颁布，中美贸易和科技战进入白热化。美国总统特朗普近日签署行政命令，以科技网络安全为由，科技战的背后是网络战，以及对网络数据的争夺。美国的国家级网络部队正试图通过开展科技战打压华为，获取 5G 时代对网络数据的截获和监听。当今网络时代所应对的对手不仅是病毒、木马、诈骗短信，更多的是其他国家的网络战部队。网络战的表现形式也不仅限于 DDOS 攻击，而是潜伏在对手网络中数年，等待时机将网络攻击至瘫痪。

宣布国家紧急状态，禁止美国企业使用对国家安全构成风险的企业所生产的电信设备。

此举明显系针对华为公司而来，华为是电信设备制造商，连续多年居大陆民营企业第1名，近期已超越美国苹果，成为仅次于韩国三星的第2大智慧手机制造商，跻身全球5G科技领头羊。该项禁令不仅仅是中美贸易和科技战的白热化，更是事关中美在关键领域统治地位的较量。

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。

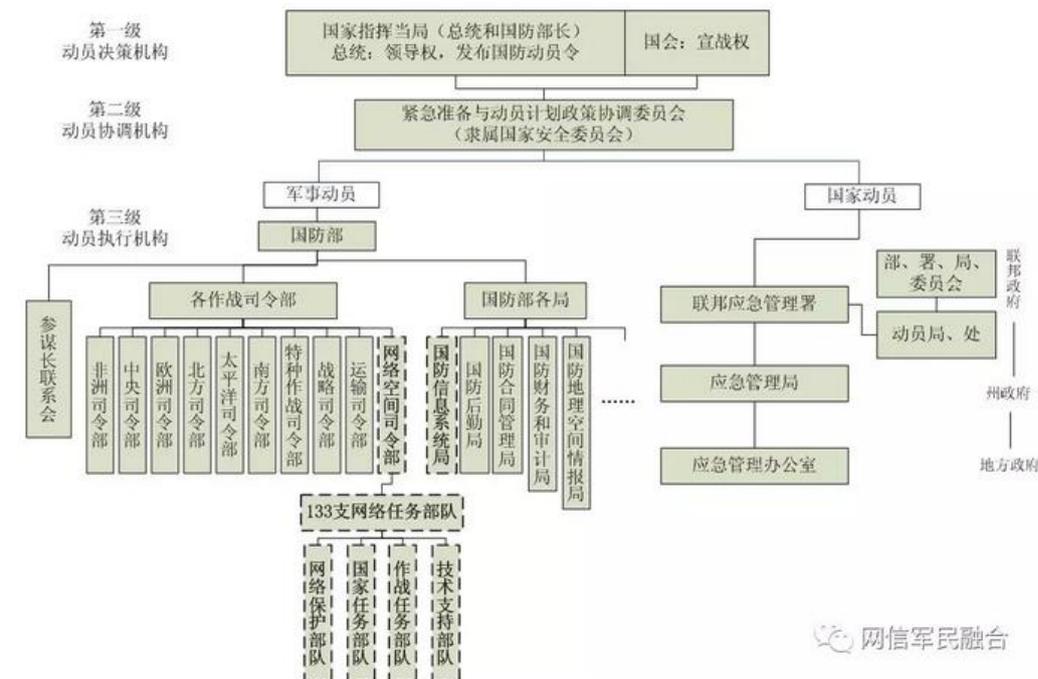
表 1：美国网络空间国防发展轨迹

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元人民币，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。

图 8：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
2017 年	德国	网络信息空间指挥部
2017 年	新加坡	国防网络署

资料来源：《网信军民融合》、东兴证券研究所

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	俄罗斯	信息作战部队
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

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。

未来，网络战的重要职责之一是情报战，即国家情报机构和网络战部队通过网络攻击方式入侵电脑获取文档，对另一个国家发起的渗透和情报窃取。

在物联网时代，网络攻击伤害将更大。由于每一个设备都有小的操作系统，都可能有漏洞，进而成为被攻击的一个要点。而物联网的攻击力度、防守难度将比电脑发起的攻击增加很多倍，所有网络虚拟空间的攻击都可以变成物理世界的伤害，例如电站断电、高铁停运、发布不实消息等。

2.2 日美芯片战“上下半场”的前车之鉴

2.2.1 上半场：自给自足的企业制度，日本政府的强势助推

上世纪五六十年代，当美国的电子厂商向日本推销电子产品时，日本几乎没有电子产业。于是，日本决定赶超。到了70年代，日本在电子产业开始与美国抗衡，其产品质优价廉，深受美国消费者欢迎。美国的电子产业受到严重打击，尤其是芯片工业，甚至出现大量亏损，于是美国决定反制。

日本电子产业迅速崛起的秘诀是：严格的市场保护，强大而全面的电子财团，政府推动民族产业的技术开发与合作。随着松下、日立、索尼等龙头企业的崛起，日本企业在国际市场上的份额急剧上升，日本电子产品风靡世界，开始在全世界挑战美国。当时两国电子产业拥有截然不同的发展模式：

- **美国科技公司（硅谷）发展模式：以市场为导向，效率高，但体量小，公司之间整合资源难。**通过风险投资为创业公司注入资金，创业公司获得资金支持后，进行持续的技术创新获得市场，提升公司估值，然后上市，风险资本卖出股票获利退出。
- **日本模式：集中力量办大事，扭转日本企业在国际竞争中孤军奋战的困局。**1974年，日本政府批准“超大规模集成电路（俗称半导体芯片）”计划，确立以赶超美国集成电路技术为目标。随后日本通产省组织日立、NEC、富士通、三菱和东芝等五家公司，要求整合日本产学研半导体人才资源，打破企业壁垒，使企业协作攻关，提升日本半导体芯片的技术水平。

“半导体芯片”计划实施4年后，日本取得上千件专利，缩小了和美国的技术差距。日本政府推出的贷款和税费优惠等措施，也让日立、NEC、富士通等企业兵强马壮，弹药充足。现代化的半导体存储芯片制造工厂在日本拔地而起。

随着生产线的日夜运转，日本发起了饱和攻击。1980年，攻下30%的半导体内存市场，5年后，日本的份额超过50%，将美国甩在身后。日本的存储芯片不仅量大，质量也很好。1980年代，美国半导体协会曾对美国和日本存储芯片进行质量测试，结果发现美国最高质量的存储芯片比日本最差质量的还要差。

在日本咄咄逼人的进攻下，美国的芯片公司兵败如山倒，财务数据每况愈下。1981年，AMD净利润下降2/3，国家半导体亏损1100万美元，次年英特尔被迫裁掉2000名员工。1985年英特尔缴械投降，宣布退出DRAM存储业务，这场战争使其亏损1.73亿美元，为上市以来的首次亏损。同时，富士通打算收购“硅谷活化石”仙童半导体公司80%的股份。硅谷的科技公司成立了半导体行业协会（简称SIA）来应对日本人的进攻，经过几年游说，成果如下：将资本所得税税率从49%降低至28%，推动养老金进入风险投资领域。但政府回应美国是自由市场，政府权力不应染指企业经营活动。

2.2.2 下半场：《美日半导体协议》攻击日本电子产业核心

随着美国芯片公司财务数据每况愈下，SIA提出“国家安全说”（美国半导体行业削弱将给国家安全带来重大风险）说服政府权力染指企业经营。由于超级武器技术离不开超级电子技术和半导体技术，但由于美国半导体技术的落后，美国军方将被迫在关键电子部件上使用外国产品包括日本货。外国货源具有巨大的不可靠性，战争时期会对美国断货，非战争时期还会向美国对手苏联供货，因此美国放任日本在半导体芯片领域称霸，就等于牺牲国家安全。“国家安全说”让美国政府醍醐灌顶，快马加鞭回击日本半导体市场。

扭转局面。1986年春，日本被认定只读存储器倾销；9月，《美日半导体协议》签署，日本被要求开放半导体市场，保证5年内国外公司获得20%市场份额；不久，对日本出口的3亿美元芯片征收100%惩罚性关税；否决富士通收购仙童半导体公司。美国人这波操作至少开创了两个记录：

- 第一次对盟友的经济利益进行全球打击；
- 第一次以国家安全为由，将贸易争端从经济学变成政治经济学问题。

随着《美日半导体协议》的签署，处于浪潮之巅的日本半导体芯片产业掉头滑向深渊。日本半导体芯片产业从1986年最高40%，一路跌跌不休跌到2011年的15%，吐出一半的市场份额，其中的DRAM受打击最大，从最高点近80%的全球市场份额，一路跌到最低10%（2010年），回吐近70%。和美国的这一战，日本此前积累的本钱基本赔光，举国辛苦奋斗十一年（从1975年到1986年），一夜被打回解放前。但由于硅谷超过7成的科技公司砍掉了DRAM业务（包括英特尔和AMD），日本人吐出的肉，并没有落到美国人嘴里，1986年之后，美国的市场份额曲线一直徘徊在20%左右。

日本电子产业的高速发展，核心是得益于自给自足的企业制度，以及日本政府的强势助推。这样的完整产业链直接限制了国外企业投资进入。而美国的协议就是在攻击日

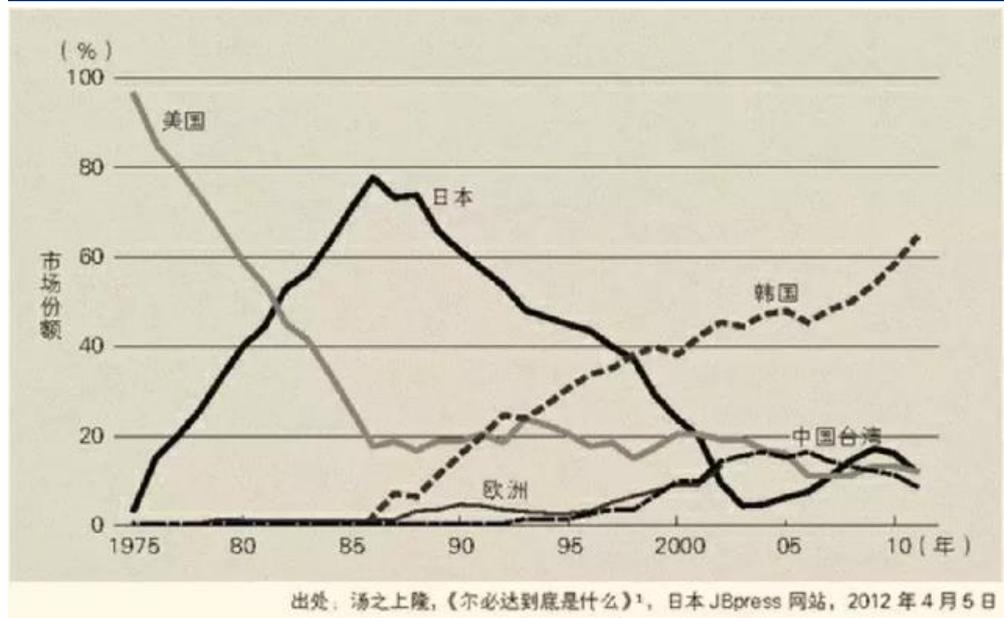
本电子产业的核心。在这个原则协议上，日本轻易而不自觉地做出了重要的战略让步。这一让步，抽走了日本电子产业优势的体制和政策的合理性，导致如日中天的日本电子产业忽然失去了坚实的基础。

同时，在签署《美日半导体协议》、丢失半导体芯片市场份额后，日本芯片厂商选择抱团取暖迎接产业复苏，陷入加拉帕戈斯化。【加拉帕戈斯化效应，是指在孤立的环境（日本市场）下，独自进行“最优化”，而丧失和区域外的互换性，面对来自外部（外国）适应性（泛用性）和生存能力（低价格）高的品种（制品/技术），最终陷入被淘汰的危险。】据当时《日本经济新闻》报道，包括 NEC、三菱电机、东芝和富士通在内的日本 11 家大型电子企业决定，共同出资设立生产下一代芯片的合资公司，以便在国际市场上与咄咄逼人的美韩等国共同竞争。

类似情况在 2005 年也曾出现，当时的日本芯片业不仅增长速度慢于全球水平，份额也不断下滑。继松下、三洋相继宣布大规模裁减半导体部门员工后，日本第三大半导体生产商 NEC 电子公司也难逃厄运，股价曾一度创历史新低。不久，东芝、日立以及瑞萨科技三家日本公司又宣布成立芯片联盟，共享半导体生产资源。联盟研究了如何通过合作提高芯片产量，合理配置旗下工厂资源。三家公司也考虑了建立一家新合资半导体公司的可能性。

而日本丢失的半导体芯片份额，几乎都进了以三星为首的韩国企业嘴里。三星 1990 年代面临美国发起的反倾销诉讼，而后巧妙利用美国人打压日本半导体产业的机会，派出强大的公关团队游说克林顿政府，指出竞争者的减少将进一步抬高美国企业购入芯片的价格，对于美国企业将更加不利。于是，美国仅向三星收取了 0.74% 的反倾销税，日本最高则被收取 100% 反倾销税。随后，三星的 DRAM “双向型数据通选方案” 获得美国半导体标准化委员会认可，成为与微处理器匹配的内存，日本则被排除在外。三星顺利搭上微处理器推动的个人电脑时代快车，领先日本企业。

图 9：1975-2010 年全球半导体市场份额变动图



资料来源：互联网，东兴证券研究所

纵观日美芯片战，市场份额的多寡不构成主要实力因素，是否掌握重组全球产业链的能力才是贸易战中决胜的关键。日本的半导体芯片企业直接被韩国企业替代。美国实际上是联手韩国，重组了全球半导体产业供应链，将日本人从供应链上抹去，使一支在全球看起来不可或缺的产业力量消失得干干净净。

2.3 中国内需市场庞大，制造业独具优势

现在美国仍试图利用国家安全理由对付中国。比日本幸运的是，中国有一个庞大的内需市场。美国想通过极限施压的封锁策略击垮华为和中国的半导体芯片行业，无疑将对其自身的芯片和软件业带来歼灭战式的打击。

20年前，美国还是世界通信业的领导者，朗讯和摩托罗拉等是世界上最杰出的通信设备和手机提供商。但是短短十多年间，随着中兴华为的崛起，美国通信业已经全军尽没，所有通信设备厂商完全退出了竞争。只有新兴的苹果手机还在凭借乔布斯的神力独撑门面。曾经在通信设备领域兴旺过的英国（马可尼）、德国（西门子）、法国（阿尔卡特）、以色列、韩国、日本等全都退出了竞争的行业。今天还有资格出现在这个领域的国家只剩下三个：中国（华为、中兴）、瑞典（爱立信）、芬兰（诺基亚）。

在2010年超越美国之后，中国成长为全球头号制造业大国。中国2010年的制造业增加值总额接近3万亿美元，约占全球制造业增加值的四分之一。尽管中国拥有庞大的制造业基础规模，但中国经济的复杂性在全球排名第26位，在制造业复杂性方面仍有改善空间。中国制造业的独有优势：

首先，中国制造业规模大、门类齐全、层次多样且高度集聚。

完整的产业链与制造体系，可以使产业变革期的各类创新迅速地、低成本地、便利地转换为产品和产业化。在云计算、人工智能、区块链等新兴数字技术的发展上，各国的差距并不大，而丰富的创新场景、庞大的创新需求，有可能使得中国在这些关键数字技术上快速突破、率先形成市场规模。

其次，中国大规模、多元化、层次丰富的需求市场，为中国制造转型升级提供了难得的“战略纵深”。

中国市场需求旺盛，且层次丰富，从高端到低端，每一消费层级都有着庞大的需求，能够为新技术、新产品、新模式的推广提供必要的规模门槛。此外，庞大的市场中不同发展阶段的企业对生产装备自动化、信息化和智能化的各类需求，将长时间同时并存，为升级提供了广阔空间。需求差异化也可以提供丰富多样的应用场景，便于企业充分试错、快速迭代，进行场景化创新。近年来，中国快速迭代的场景化创新已经成为一大特点，创新形成市场规模的速度大大提升，显著增强了中国的经济活力。

大数据、云计算、物联网、人工智能等数字化技术发展风起云涌，与制造业深度融合，深刻影响着整个产业结构和经济社会。充分发挥上述优势，中国就有可能最先演进出一个用工业互联网连接的、辐射全球的新制造网络。抢抓新一轮产业革命大潮所带来的机遇，实现中国制造业由大到强，正是以5G为核心的新一代网络所需承接的历史

使命。依托庞大的国内市场和完整的产业链布局，叠加政府政策支持和成立集成电路大基金的资金支持，中国半导体行业有望抗住这次中美科技战的冲击。与日美芯片战不同的是，日本签订《美日半导体协议》后日本是被迫打开国内 20% 以上的市场份额，而此次中美科技战在国内庞大市场和完整产业链布局情况下，美国竟主动让出我国国内的芯片市场，对我国半导体行业是一个天大的利好。所以我国半导体产业有望凭借接管美国禁运后的对芯片产品的需求缺口，而不是步日本后尘。

3. 科技赋能服务业，本土供应商崛起，是我国保持经济高速增长 的必然需求

3.1 改革开放、科技创新提升服务也效率，迎接经济高收入阶段关键挑战

3.1.1 高收入阶段关键挑战：提高服务业的劳动生产率

目前，中国走向高收入阶段供给侧改革的重点和现阶段面临的关键挑战，就是产业结构的调整和劳动生产率的提高。中国经济到今天有了长足的增长，但同时面临着中等收入陷阱的问题。随着人均收入从 1978 年的 160 美元到现在的 10000 美元，这一典型的中等收入陷阱的入口，GDP 增长速度自 2012 年以后逐渐下滑到现在的 6% 以上。所以中国经济面临最大的宏观挑战就是人均增长速度能不能稳住，人均 GDP 能不能持续增长。今后五年中国经济的发展决定了未来五十年，也会决定世界经济未来十年、二十年的经济发展。

中国在结构转变上和世界的整个结构转变是完全一致。从世界发展结构变化角度来看，在此关键点，典型的结构性变化模式是：农业就业占 GDP 比重下降，工业先上升后逐渐下降，服务业普遍不断提高。中国在结构转变上和世界的整个结构转变是完全一致的，2013 年以后中国的服务业逐渐超过工业，占比 50%，而工业的比重逐渐下降。

但中国的结构转变也存在问题。将工业劳动生产率除以服务业劳动生产率，当值为 1 时，表示二者相同。但在进入 2000 年以后，我国工业进入高科技的工业时代，工业劳动生产率的速率提高很快，目前工业劳动生产率是服务业劳动生产率的 120%。因此，当我们不断提高服务业比重时，提高一个百分点服务业比重，就意味着丢掉二十个百分点的劳动生产率。如果这个格局继续下去，工业劳动生产率的增长速度一定会下降，这也是全世界在过去 50 年、80 年的经验。因此，提高服务业的劳动生产率，成为了最大的挑战。

服务业可被分为两类：市场化的服务业和非市场化的服务业。市场化的服务业，如金融业、酒店业都是市场化服务业，大部分的教育、医疗、政府活动都是非市场化服务业。通过大量数据分析，在 2000 年后，市场化服务业的劳动生产率在不断提高；而非市场化的服务业进展非常缓慢，差距非常大。所以，提高非市场化的服务业成为很重要的一部分。

目前，我国金融业、商业零售和电商的劳动生产率高于世界平均水平，有很高的电商比重和领先的服务。但是，信息和计算机服务业，称为商务服务业，在中国特别不发达，这两块服务业的劳动生产率特别低。而健康和教育则远远低于劳动生产率的世界一般水平。即非市场化的服务业依然很低。

要提高服务业劳动生产率，就要继续改革和开放。从去年总书记在博整会上宣布后，我国的服务业现在正在面临一个大规模的开放，进一步的金融改革，服务业、文化产业、医疗卫生、教育对外开放等。目前，金融、教育、文化、医疗等服务业有些开放，设计、审计、物流、电子商务等服务业正在开放，电力、民航、铁路、石油等公用的服务业都在开放，构成改革和开放的重要组成部分。市场化的改革和开放将称为提高服务业劳动生产率的重要方面。

3.1.2 科技赋能：人工智能颠覆制造业、服务业、军事

在当今复杂环境下，仅有改革开放并不够，还要加上科技的力量。因为当劳动生产率差距如此之大的时候，就需要科技的力量赶上制造业水平，来维持经济增长的速度和稳定。因此，人工智能会起很大的作用，正在颠覆未来，几乎改变了所有制造业和服务业、军事，改变物质和财富的生产和分配。

当前，制造业进入三个维度的数字化过程：

- **第一，垂直维度。**开始能够把制造业从生产车间平面产生的数据，汇总到财务、战略和云，每一分钟都在产生无数的数据。第一次有海量的实际生产线数据，改变了整个产过程；
- **第二，供应链管理。**供应链管理是一件非常重要的事情，其效率和迭代改变了整个产品质量。300多家供应链企业都在深圳一个小时内车程之内，可以每周一次会议，通过人工智能网络不断迭代，不断创新出新产品。
- **第三，制造业的三维空间管理和自动化。**产品在开始生产的同时，会出现一个虚拟的产品生产过程。实体产品在生产的过程中，虚拟产品根据两维信息不断更新和设计自己，因此生产的过程就是新产品的的设计过程。制造业的三维变化产生了巨大的发展空间。

未来制造业提供劳动生产率的空间是巨大的。制造业的自动化是一个庞大的过程，韩国拥有最高的每万名工人机器人数量，高达530个；中国却只有22个，而中国制造业是全世界最大的。2004年时，中国制造业仅与德国相等，而今年中国制造业是美国日本和德国的总和。因此，未来制造业提供劳动生产率的空间是巨大。与此同时也给服务业创造了更大的压力，需要服务业的猛追。

- **物流，是一个典型的服务业劳动生产率。**目前，物流从生产地到客户的整个过程自动化程度非常高，有完全自动化的仓库、库存。消费者所能看到的外卖小哥、快递小哥仅占整体物流产业链的7%。未来，物流是一个12万亿人民币，占GDP15%的市场。
- **金融，人工智能不仅仅是第三方支付，而在执行理财、交易、配送中的完全人工智能化。**金融科技动金融业在存款、贷款、支付、融资、投资管理的转变和颠覆是巨大的。
- **医疗，是一个巨大的、开放还很不够的服务业。**人工智能在远程护理、诊断、支持、风险评估、研发、管理、营销上的应用非常广泛。将医疗人工智能业务分类，在远程预防和护理业务上，已有许多企业可以做得很好；影像识别、医疗方案、研发的应用也已经很普遍。然而，人工智能在医院运营优化和营销上的应用反而很少；可以解释的原因是，医院目前还不完全市场化运作，因此其技术化和现代化也就比较落后。

综上，人工智能对整个宏观经济的影响是很大的，是中国现阶段跨越鸿沟的关键点非常重要的条件。到 2035 年，可以让中国 GDP 增速从 6.3% 提高到 7.0% 左右。中国在人工智能方面已有深厚的基础，主要的人工智能企业有金融、安防、无人机、家居、医疗、客服、个人助理、互联、无人驾驶、机器人十个主要的行业，分成应用、技术和基础来看。目前，在计算机视觉、语音识别、云计算等方面技术开始领先，以阿里为首的三大巨头在世界上具有较强的竞争力。我们的强项在应用，也逐渐在技术层面有所突破；需求端好与供给端的不平衡也不断得到改善。

人工智能最大的特点是能够规模推动技术，成为创新和赶超的新的途径。在中国电商在整个商务比重上超过美国后，由于规模带来效率，现在阿里巴巴每秒的支付处理速度是美国最快速度的 3 倍到 4 倍，即是规模带来的技术。

国务院发文强调人工智能的战略目标，2020 年同步，2025 年领先，2030 年成为世界中心。依托人工智能战略，支持改革和开放，提高服务业劳动生产率。目前我们面临着最关键的五年，不仅是供给侧改革的五年，也是市场化开放和科技化发展的五年。中国正在迈入高收入阶段，关键是劳动生产率的提高，迎接挑战，我们需要继续改革开放、加快科技的发展。

3.1.3 “5G 技术”赋能各行业

随着 5G 技术的逐步成熟，5G 技术将推动移动互联网、物联网、大数据、云计算、人工智能等关联领域裂变式发展，在制造业、农业、金融、教育、医疗、社交等垂直行业将赋予新应用。

(1) 制造业

5G 技术可以帮助制造业的生产操作变得更加灵活和高效，同时提高安全性并降低维护成本。这将使制造商能够增强利用自动化，人工智能，增强现实和物联网的“智能工厂”。可以通过 5G 移动网络远程控制，监控和重新配置受人控制和不受人控制的机器人。这将使机械和设备通过自我优化，简化生产，规划，供应链物流甚至产品开发来改进流程。下一代无线技术也可能推动增强现实(AR)的应用，因为 5G 网络提供持续增强图像质量所需的高带宽和低延迟。在工厂环境中，这意味着 AR 可以支持培训，维护，施工和维修。

例如，位于爱沙尼亚塔林的爱立信工厂采用 AR 进行故障排除，以帮助降低故障成本并减少生产停机时间。三星和 AT&T 合作在德克萨斯州奥斯汀创建了美国首个以制造业为主的 5G“创新区”。该测试场旨在展示 5G 如何影响制造业。

(2) 能源与公用事业

5G 可以为能源生产，传输，分配和使用带来创新的解决方案。它还有望带来下一波智能电网功能和提高效率。5G 技术可以通过低成本联网集成许多未连接的耗能设备。这将改善电网监测并使预测能源需求更加准确。通过更多连接的智能电网，能源管理将变得更加高效，从而降低电力峰值和整体能源成本。此外，5G 显著延长了电池相关设备的使用寿命，有时长达 10 年。这使得物联网传感器的大规模部署成为能源行业更实用的解决方案。例如，泄漏检测器可以沿管道放置，允许连续监测，可以防止破坏性泄漏并减少人为干预的需要。这也将提高安全性。5G 还支持使用无人机监控和维护生产资产的传输，从而改善电网正常运行时间。仅此一项就可以使成本降低 30%。

(3) 农业

世界各地的农民正在使用物联网技术来优化农业过程，如水管理，灌溉施肥，牲畜安全和成熟度监测，作物交流和空中作物监测。5G 技术可以促进物联网设备的采用，从而实现这一目标。5G 可以为农民提供实时数据，以监控，跟踪和自动化他们的农业系统，从而提高盈利能力，效率和安全性。在农业等高风险行业，这些产量和精度的提高至关重要，特别是当气候变化给全球农民带来新的威胁时。例如，在英国，大约 80% 的农村地区 4G 范围之外。在美国，截至 2015 年，农村地区超过一半的美国人无法使用宽带服务。

(4) 医疗

5G 可以通过多种方式改善全球医疗保健，同时提高医疗行业的效率和收入。据估计，在医疗保健领域使用 5G 技术将在 2026 年创造 76 亿美元的收入机会。医疗系统需要更快、更高效的网络来跟上它处理的大量数据，从详细的患者信息到临床研究，再到高分辨率的 MRI 和 CT 图像。预计到 2020 年，医疗行业将产生大约 2.314 千万亿千兆字节的数据。5G 的低延迟可以在不降低网络速度的情况下传输大量数据。

5G 还可以使远程监控设备(如可穿戴技术)在将患者健康数据实时发送给医生的同时，拥有更长的电池寿命。医疗保健提供商可以将这些数据与环境数据(例如空气质量)相结合，通过围绕患者所在地的 5G 物联网传感器收集，以创建更全面和适应性的护理方法。

远程机器人手术也可以改善。由于这些过程需要高清图像流，因此低延迟和高吞吐量通信至关重要。5G 网络可以促进远程手术程序，因为它们可以实现无滞后和超快速连接。

(5) 运输

将公共和私人车辆与 5G 联网可以改变人们和货物在世界各地旅行的方式。从公共巴士到私人物流车队，5G 技术可以提高运输系统的可视性和控制。随着 5G 网络变得越来越普遍，城市将获得对其运输系统的实时，端到端可视性的访问权。5G 可以增强车辆与车辆(V2V)的通信，这是改善在新兴的无人驾驶世界中道路安全的关键组成部分。

然而，V2V 通信必须实时进行，因为毫秒可能会导致近距离呼叫和致命碰撞。实现这种高速互连需要车辆在彼此之间传输大量数据而没有任何滞后。5G 网络可以通过其可靠性和低延迟实现这一目标。

5G 还可以在车辆与基础设施(V2I)通信中发挥关键作用。V2I 通信将车辆与交通信号灯，公交车站甚至公路本身等基础设施连接起来。这可以改善交通流量，减少外部危险因素，增加车辆反应时间，提高公共交通效率。

(6) 金融服务

随着金融机构越来越关注移动运营，5G 技术有望加速从内部运营到客户互动的数字化。其带来的安全性和速度的提高可以让用户立即在他们的设备上支付交易，比现在的任何流程都要快得多。5G 还可以使远程出纳成为可能。这将使客户能够通过视频会话获得个性化关注，而无需前往银行的分支机构。

5G 联网可以允许可穿戴设备与金融服务共享生物识别数据，以便立即准确地验证用户身份。这可能导致生物特征认证中的误报减少。5G 技术还可以为新的基于人工智能的个人银行服务铺平道路，这可以根据用户的消费习惯为用户提供财务建议。

（7）保险

5G 可以帮助保险公司全面做出更有效，更有把握的决策。该技术可以使保险公司实时跟踪货运，改变保险公司评估商业和海上保险的方式。通过更有效的数据共享，健康和人寿保险公司可以在提供报价时做出更明智，更准确的决策。随着可穿戴的 5G 连接医疗保健设备的普及，健康保险公司可以提供“积极强化”政策，如果维持一定程度的活动或健康，保费将会降低。随着 5G 迎来自动驾驶和无人驾驶车辆的新时代，实时数据和报告可以在客户意外发生后立即发送给汽车保险公司。这将允许汽车保险公司更有效地调查和解决索赔。

（8）云计算

由于移动设备的低吞吐量，高延迟和不一致的连接性，云应用程序在功能和特性方面经常被淡化。**5G 网络可以提高基于云的应用程序的响应能力，可伸缩性和灵活性。**移动应用程序可能比以往更加复杂。5G 的超低延迟和高吞吐量将使云计算体验与桌面企业 LAN 连接相媲美、甚至是最佳。它甚至可以增强当今的云计算功能，这些功能通常仍会遇到延迟问题和网络可访问性问题。

（9）旅游业

5G 正在为“智能旅游”概念的出现提供无线基础设施。它可以吸引更多的游客前往目的地，并为他们提供更多身临其境的体验。许多旅游组织已经在研究和开发 5G 连接技术，以改善其旅游目的地。例如，英格兰西部联合管理局已经为巴斯和布里斯托尔的主要旅游景点提供了 500 万英镑的奖励，用于试验 AR / VR 体验。BBC, Aardman 和布里斯托尔大学将致力于该项目的内容和技术开发。

（10）公共安全

5G 可以增强公共安全能力，从而缩短应急响应时间。通过 5G 网络，诸如实时视频，安全通信和媒体共享等应用可用于在紧急情况下协助第一响应者。面部识别和车牌扫描也可以得到显著改善。5G 网络可以改善公共安全社区内的信息共享，通过身体监控，无人机，群聊，文件共享和位置共享实现安全可靠的视频共享。5G 和物联网技术还可以推进指纹传感器，这有助于识别罪犯或受害者。在灾后情况下，5G 连接的无人机将能够提供救援物资并协助寻找失踪人员。增强的传感器，摄像头和其他自动化设备网络将有助于更全面地了解任何公共安全情况，从而有可能使世界各地的城市更加安全。

（11）车联网

车联网价值链中的主要参与者包括：汽车制造商、软件供应商、平台提供商和移动运营商。移动运营商在价值链中极具潜力，可探索各种商业模式，例如平台开发、广告、大数据和企业业务。

传统汽车市场将彻底变革，因为联网的作用超越了传统的娱乐和辅助功能，成为道路安全和汽车革新关键推动力。驱动汽车变革的关键技术—自动驾驶、编队行驶、车辆生命周期维护、传感器数据众包等都需要**安全、可靠、低延迟和高带宽的连接**，这

些连接特性在高速公路和密集城市中至关重要，只有 5G 可以同时满足这样严格的要求。5G 有可能成为统一的连接技术，满足未来共享汽车、远程操作、自动和协作驾驶等连接要求，替代或者补充现有连接技术(例如目前正在美国被授权使用 V2V 技术的 5.9GHz DSRC)。

3.2 华为：为本土供应商带来巨大自主可控机会

3.2.1 海思芯片版图完善，本土供应链崛起

海思半导体卧薪尝胆，十几年积累扩大华为芯片版图。自 2004 年海思半导体成立开始，华为就不断加强的核心技术研发积累，包括芯片、操作系统等硬核科技。而其研究经费中，有 40%都投在了芯片上，得到很多成果。包括不逊色于高通旗舰芯片的麒麟 980、5G 基带芯片巴龙 5000、AI 芯片昇腾系列、服务器芯片鲲鹏系列等。另外，在视频应用上，海思也有全系列的机顶盒芯片和电视芯片、安防芯片等。尤其是安防芯片，早在 2014 年，海思已占领全球半数以上的市场，国内市场占有率达 90%，安防龙头海康威视、大华股份的关键芯片都由华为供货。整体来说，经过十几年的积累，华为的芯片家族已相当庞大，包括光网络芯片、数据通信芯片、接入语音芯片、高端路由器、交换机芯片、模拟芯片、GPU 图像处理器等，绝大部分产品都已经能够自主开发。

中兴事件后加大库存，加快研发进度，调整零部件供货商。自去年中兴事件以来，华为就开始加大库存备货，从 6-12 个月的备货周期增加到 1-2 年。从去年 4 月到今年 5 月，整整一年有余，给了华为上下充足的时间去增加库存，以加快研发进度、调整零部件供货商，获得喘息的机会。

本土国产供应链的崛起，华为事件给了本土供应商一个巨大的市场机会。中国本身是一个半导体消费大国，消费占全球比重约 43%，但目前的自给率只有约 10%。自给率低的原因是先天不足加上中国市场的全面开放。由于美国半导体产业发展较早、技术领先，我国企业在选用元器件的时候，必然会优先考虑技术先进的美国产品。导致了本土企业市场份额处于劣势，没有充足的资金投入先进技术的研发。但经过几十年的发展、积累，本土供应链即使技术差了点，在产品体系的完备性上并不差，华为事件给了本土供应商一个巨大的市场机会。2018 年，华为芯片采购金额超过 210 亿美元，是仅次于三星、苹果的全球第三大芯片买家；华为的芯片采购支出金额同比增长了 45.2%，是全球前五的买家中增速最快的。此外，同期的联想、小米、步步高（包含 VIVO 和 OPPO），均跻身全球十大芯片买家之列。当美国制裁华为，中国企业转向支持本土供应商成为必然。自从这次事件后，华为主动邀请本土供应商参与底层技术的共同研发，将成为我国高端制造产业升级的上甘岭战役。中国市场的庞大规模、本土供应链的底蕴，都将带给华为，以及其他中国科技公司无比的韧性。

3.2.2 华为优质备胎盘点

2018 年 11 月，华为在深圳举行核心供应商大会，邀请 150 家供应链企业到场，并对 92 家供应商进行了表彰。在所有获奖供应商企业中，美国公司多达 33 家，其中英特尔、NXP 是连续十年的金牌供应商，大陆公司共有 25 家，日本公司有 11 家。在大陆的 25 家供应商中，上市公司超过 15 家，除了物流类合作伙伴（顺丰）外，主要有以下几类：

表 4：华为 25 家大陆供应商盘点

企业类型	名称
手机组装的企业	比亚迪电子
生产 PCB 板的企业	生益科技、沪电股份、深南电路（基站 PCB）
生产线缆、光纤的企业	中利集团、长飞光纤、亨通光电
生产光模块的企业	光迅科技、华工科技
生产显示面板的企业	京东方、深天马
生产连接件，其他模块的企业	立讯精密（连接件）、歌尔股份（声学）、蓝思科技（前后盖玻璃），欧菲光（摄像头及屏下指纹模组）

资料来源：公司官网，东兴证券研究所

除此之外，从 33 家美国公司的核心产品入手，盘点华为的备胎。

第一层级的，包括 CPU、通讯芯片、操作系统等。属于核心关键技术，研发门槛高，只能交给华为海思去攻关。

第二层级的，包括 FPGA 芯片、模拟芯片、数字信号芯片、存储芯片、传感器等应用芯片，和数据库、EDA 工具等应用软件。属于次一级的关键技术，我国的相关供应链较弱，但也不是没有。

第三层级的，包括光器件、连接器、PCB 板、零组件和测试服务等。这块的门槛最低，我国也有较成熟的供应链，进口替代最容易实现。因而，在最近的华为概念股炒作中，第三层级的公司最受关注。

表 5：华为的 33 家美国供应商

层级	内容	公司名称
第一层级	CPU 芯片	英特尔
	通信芯片	高通
	操作系统	微软
第二层级	FPGA 芯片	赛灵思
	模拟射频和数字信号芯片	博通、德州仪器、美满、亚德诺、康沃、安森美、思佳讯、Qorvo
	存储芯片	美光、希捷、西部数据
	传感器	赛普拉斯
	应用软件	甲骨文、红帽、新思、Cadence、风河
	光器件	新飞通、高意、Lumentum、菲尼萨
	连接器	安费诺、莫仕
第三层级	PCB 板	迅达
	芯片组件	Inphi、迈络思
	测试服务	是德、思博伦
	保险服务	AIG 保险

资料来源：公司官网，东兴证券研究所

短期来看，第三层级的四个环节：光器件、连接器、PCB 板、测试服务备受关注，短期直接受益。如中际旭创、光迅科技、立讯精密、深南电路、生益科技等，大多在一季度的 5G 行情中受益匪浅。

长远来看，第二层级的发展将决定本土供应链的崛起。包括 FPGA 芯片、存储芯片、模拟芯片、数字信号芯片、传感器和应用软件等。这些环节，美国在全球都享有巨大的技术优势，我国的供应链与之相比差距巨大，但已有一批星星之火。

（1）存储芯片

存储芯片领域用量巨大，进口金额以千亿美元计算，目前的主要本土企业包括紫光旗下的长江存储、兆易创新（603986）与安徽合作的长鑫存储。其中，兆易创新由朱一明创办，十几年来在细分领域 NOR Flash 的夹缝中不断突破，成长为 A 股的存储芯片龙头。

2016 年，朱一明投身长鑫存储的二次创业，整个长鑫存储项目预计总投资超过 72 亿美元，工程将分 3 期完成，预计月产能将达 12.5 万片，成为我国最大的存储芯片 IDM 工厂之一。长鑫存储目前累计已投入了 25 亿美元的研发费用，并完成了第一座 12 英寸 DRAM 存储器晶圆厂的建设，已持续投入晶圆超过 15000 片，预计在今年秋天进入大规模量产阶段。

另外，备受瞩目的长江存储项目也在稳步推进之中，进入第二阶段 2 万片产能爬坡期，目前已采购了数千台芯片设备，相当一部分都由本土供应链提供。其中，中微公司供应刻蚀设备，盛美半导体和北方华创供应清洗设备，被国资收购的 Mattson 贡献去胶设备、热处理设备等。

（2）FPGA 芯片

FPGA 芯片在云计算、数据中心中有着重要地位，全球市场规模约为 60 亿美元，中国的 FPGA 市场规模约占全球三分之一，即 20 亿美元以上，并且快速成长。我国在该环节的龙头是上海的安路科技和深圳的紫光同创。

安路科技近年来发展迅猛，2011 年成立，先后获得了中信资本、华大半导体等众多 VC 的追捧，A 股公司士兰微（600460）也是其股东之一。据安路科技销售部副总经理梁成志向媒体透露的信息，2018 年安路的销售额增长了两倍多，预计 2019 年的业绩将成长三倍，FPGA 芯片年销量将高达数百万颗。

紫光同创隶属于紫光集团，属于 FPGA 领域的国家队，发展时间较早，由于注册地在深圳，与华为有较深入的合作，据悉去年已从华为获得千万元量级的订单收入。

（3）模拟芯片

模拟芯片是一个市场规模庞大，品种繁多、产品生命周期长、注重经验积累的行业。由于行业特性所致，模拟芯片行业通常是产品种类越丰富的公司竞争力越强，比如德州仪器就拥有 10 万+的产品和 10 万+的客户。也因此，我国的模拟芯片企业被美国的博通、德州仪器等巨头打压，长期发展缓慢。

此次封锁，对本土供应链来讲将是天赐良机。A 股的模拟芯片龙头是圣邦股份，其产品覆盖信号链和电源管理两大领域，包括运算放大器、音/视频放大器、马达驱动及电池管理芯片等，涵盖 16 大类 1000 余款产品。2018 年度，公司研发费用投入 9265.86 万元，占到营收比例的 16.19%，年内推出了 200 余款新产品，并入选《电子工程专辑》等媒体评选的 2018 年度“十大中国 IC 设计企业”。

（4）传感器

韦尔股份耗资 153 亿元对豪威科技的并购案在近期已经获得证监会的通过。豪威科技是全球前三大的图像传感器供应商，在手机、汽车、安防领域的 CIS 占有率分别是全球第三、第二、第一。2015 年 5 月美国豪威被由中信资本、北京清芯华创和金石投资组成的财团以 19 亿美元收购，最终于 2016 年初完成私有化，成为北京豪威的全资子公司。2018 年 5 月，韦尔股份再次筹划收购豪威科技，并最终将其收归旗下。

(5) 功率芯片

闻泰科技收购安世半导体（估值 339 亿元）是该环节最重磅的资产。安世半导体原芯片巨头恩智浦剥离的标准件业务，从细分市场的全球排名看，二极管和晶体管排名第一，逻辑器件排名第二（仅次于 TI），小信号 MOSFET 排名第二，汽车功率 MOSFET 排名第二（仅次于 Infineon）。公司的核心下游客户包括博世、德尔福、思科、苹果、谷歌、华为、三星、亚马逊等。在数据库软件、EDA 软件等领域，也有南大通用、华大九天等企业在开拓，虽然技术上尚有差距，但基本也能用。

未来，中国产业升级终究要走上自主研发的道路，华为的本土供应链遍布高端制造的各个环节，虽是星星之火，但定能燎原。

4. 风险提示

互联网监管推进速度不及预期，中美贸易战进一步恶化的风险。

表 6：重点跟踪公司

公司名称	盈利预测				PE 估值			
	2017A	2018A	2019E	2020E	2017A	2018A	2019E	2020E
卫士通	0.20	0.19	0.65	0.96	148	156	45	31
中国长城	0.20	0.34	0.44	0.56	46	27	21	16

资料来源：东兴证券研究所

分析师简介

单击此处输入文字。

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，4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。
单击此处输入文字。

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，市场有风险，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。