东兴证券 DONGXING SECURITIES

美国对伊朗实施网络战，禁运认证申威自主CPU实力

——大安全“半月谈”第三期

2019 年 06 月 26 日

看好/维持

国防军工 | 行业报告

投资摘要：

网络战阴霾笼罩世界。日前美多家媒体证实美国对伊朗发动了网络攻击。美军打造全球最大网络武器库，攻击对象趋于泛化，且完成了从力量建设、法律制定、情报收集、网络结盟、实战检验等发动网络战争的全部准备，或将引发全球网络军备竞赛。从网络战战备的角度，当前中美冲突中网络战与科技战叠加共振，中国应对策略迫在眉睫。当前应转变防御思想，建设网络战争反导系统，开展实网攻防演练，打造国家级别安全大脑，充分利用当前新技术武装自己。

申威，保障党政军安全的“美国政府认证”CPU。近期美国又因为超算制裁了五家中国科技公司，其中的江南所缔造了大国重器南湖之光超算。而南湖之光离不开自主技术的 CPU 申威。申威系列 CPU 除了用在超算外，在众多民用领域都可应用。单核可用于物联网和嵌入式；2 核与 4 核 CPU 可用于嵌入式工控设备、桌面电脑、笔记本电脑、低端服务器、网络设备等领域；16 核 CPU 主要应用于各种高端服务器、高性能网络设备、低性能超算等领域。且申威生态持续发展，与众多产品进行了适配，产品技术日益丰富，看好申威在民用领域国产安全方面得到广泛应用。

拟态安全与互联网监管有望在等保 2.0 下打开新的市场空间。随着等保 2.0 的发布，5 月 28 日网信办发布了《数据安全管理办法（征求意见稿）》，互联网监管层面需求得到极大扩展。而在科技新基建领域，中国网安在拟态防御比赛中夺奖，网络空间拟态防御的愿景是，能够应对拟态界内未知漏洞后门等导致的未知风险或不确定威胁；拟态防御的有效性由架构内生防御机制决定而不是依赖现有的防御手段或方法；不以拟态界内软硬构件的“可信可控”为前提，适应全球化开放生态环境；能够融合现有的任何安全防护技术并可以获得超非线性的放大防御效果。此次获奖也代表了我国央企安全技术不断实现突破，网络安全能力进一步提升。

投资建议：网络战阴霾有望使我国加强网络战战备，利好网安国家队卫士通。同时互联网监管和拟态安全技术提升也有望在等保 2.0 下打开市场空间。而新一轮美国针对国产 CPU 厂商海光和申威的制裁，也反映了国产 CPU 重要性，推荐中国长城，建议关注华东电脑。

风险提示：等保 2.0 落地速度不及预期，网络安全行业发展不及预期，国产安全业务发展不达预期。

行业重点公司盈利预测

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

未来 3-6 个月行业大事：

中国长城拟收购华大半导体和中国振华持有的天津飞腾 35%股权。

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

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

目录

表格目录

插图目录

1. 网络战阴霾笼罩世界

1.1 美国对伊朗实行网络战

美多家媒体证实美国对伊朗发动了网络攻击。

6 月 23 日，俄罗斯塔斯社援引美国“华盛顿邮报”消息披露，经美国总统特朗普下令，美军对伊朗发起了报复性攻击。美国情报部门消息人士称，此次美军的报复主要是在网络空间进行，攻击的主要目标是伊朗的导弹发射计算机系统。白宫和美军网络司令部拒绝就此信息发表评论。与此同时，美国国防部官方代表 Elissa Smith 说：“作为我们政策和行动安全的一部分，我们不会讨论行动，情报活动和我们在网络空间的计划。”

另据 Yahoo News 报道，美国针对伊朗间谍组织的报复性数字攻击于周四实施。《华盛顿邮报》、《纽约时报》、美联社都用各自的消息源证实了该报道。而就在同一天，美国总统特朗普取消了对伊朗目标的空袭。

据悉，袭击的目标是一个“情报组织”，该组织要么跟伊朗革命卫队有联系或存在部分联系。Yahoo News 报道指出，该组织与最近在该地区对商业船舶的攻击有关联。《华盛顿邮报》则称，该袭击严重损害了伊朗的军事指挥和控制系统，但没有造成任何人员伤亡。《纽约时报》表示，伊朗的导弹控制系统也成为美方攻击的目标。

据了解，网络攻击由美国网络司令部发起，《纽约时报》的报道显示，这些攻击早在几周前就有了计划，意在回应针对油轮的攻击以及最近一架美国无人机被击落的事件。

实际上这并不是美国第一次卷入针对伊朗资产的网络攻击。此前，美国曾协助开发了攻击伊朗核离心机的 Stuxnet 蠕虫病毒。2016 年，曾有报道称，美国制定了一项名为 Nitro Zeus 的计划，该计划本来是用来对付伊朗的基础设施，但据报道该计划后来被搁置了。

目前还不清楚网络攻击的整体规模也不清楚其产生的影响，但未来可能还会发生更多这样的冲突。

图 1：美国有关对伊朗实施网络战的报道


CISA Statement on Iranian Cybersecurity Threats

WASHINGTON – In response to reports of an increase in cybersecurity threats, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher C. Krebs issued the following statement:

"CISA is aware of a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies. We will continue to work with our intelligence community and cybersecurity partners to monitor Iranian cyber activity, share information, and take steps to keep America and our allies safe.

"Iranian regime actors and proxies are increasingly using destructive 'wiper' attacks, looking to do much more than just steal data and money. These efforts are often enabled through common tactics like spear phishing, password spraying, and credential stuffing. What might start as an account compromise, where you think you might just lose data, can quickly become a situation where you've lost your whole network.

"In times like these it's important to make sure you've shored up your basic defenses, like using multi factor authentication, and if you suspect an incident – take it seriously and act quickly. You can find other tips and best practices for staying safe online here.

"Anyone who has relevant information or suspects a compromise should immediately contact us at NCCICCUSTOMERSERVICE@hq.dhs.gov."

###

Chris Krebs
@CISAKrebs

Read my statement on Iranian cybersecurity threats below.

♡ 145 3:49 AM - Jun 23, 2019

138 people are talking about this

网络法前沿

资料来源：公司官网，东兴证券研究所

中新网 6 月 24 日电综合报道，美国总统特朗普日前表示，24 日起将对伊朗新增重大制裁。

1.2 美国此举有望引发全球网络军备竞赛

打造全球最大网络武器库，美国将引发全球网络军备竞赛。挖掘软件和系统漏洞、开发木马病毒，用于网络攻击甚至网络战。美国军队和情报机构正通过打造堪比核武的全球最大网络武器库，在全球引发网络军备竞赛。截至 2016 年底，中央情报局直属的网络情报中心拥有超过 5000 名员工，总共设计了超过 1000 个木马、病毒和其他“武器化恶意代码”。除了美国国家安全局、中央情报局，美军网军也在开发自己的网络武器，美国开发的网络武器多达 2000 种，是世界上头号网络武器大国。

种类丰富的网络武器，不仅帮助美国国家安全机构进行网络攻击行为，也助其窃取国家情报和商业信息等敏感信息。目前业界认为是灭霸级别的两个高级持续性威胁（APT）组织：“方程式”和“索伦之眼”，其后台都是美国国家安全局（NSA）。“方程式”组织在 2000 年到 2015 年间，对全球 43 个国家和地区的上万台主机实施了 APT 攻击，中国受攻击数量列于全球首位。“索伦之眼”主要针对中国、俄罗斯进行网络间谍活动，以窃取敏感信息为主。在针对中国地区的攻击中，有上百个计算机终端受影响。

日前，美国空军向美国网络司令部交付了第一代重要的新型网络平台，国防部官员称，此平台可以向网络团队提供重要工具，加强协同性。美国空军正在开发的“统一平台”代表了一种联合力量，它可以让网络部队共享信息，执行任务计划，及提供网络任务执行所需的命令与控制。

美国加快网络空间备战计划，网络战争将再次升级。去年，美国国防部发布的网络空间战略强调了“前沿防御”(Defense forward）理念。这被外界解读为美国军方将在他国，而非美国本土实施网络攻防行动。此前，美国总统也赋予军方不受阻挠地部署先进网络武器的自由。作为网络战的始作俑者，美国发起了首例使用网络武器攻击他国设施的行动，它不仅是网络战最强的国家，也是发动网络战最多的国家。美国在网络空间的备战计划从未停歇，目前，美军拥有 133 支网络战部队。2006—2016 年 10 年间，美军先后举行的大规模“网络风暴”演习或者网络太空战演习共 7 次，其中 3 次网络攻防作战行动专门针对中国。

表 1： 美国在网络空间的备战计划从未停歇，多次发动网络战争

时间	网络战争
2004	美国发起网络攻击，导致利比亚国家顶级域名瘫痪
2010	美国和以色列联合制造的“震网”病毒攻击伊朗核设备，致使伊朗核计划几乎“停滞”
2016	美国前国防部长卡特首次承认，美国使用网络手段攻击了叙利亚，ISIS 组织等
2018	美国总统特朗普签署命令，推翻了前总统奥巴马 2012 年签署的“第 20 号总统政策指令”(PPD-20)，让军方更自由地部署先进网络武器，而不用受国务院和情报界阻挠。

资料来源：公开资料整理，东兴证券研究所

美国滥用网络能力，攻击对象趋于泛化。美国作为全球网络空间事实上的超级霸主，网络攻击能力、网络情报获取能力首屈一指，其滥用网络攻击能力，扰乱网络空间秩序的行径从未停止。特朗普任职期间，出台了新版的“国家网络战略”，强调利用主动防御和攻击手段来遏制各种可能的网络攻击，降低对手发动网络攻击的意图和能力，必要时可采取先发制人的网络攻击。美国于 2018 年中期选举时，允许相关部门对俄罗斯发动网络攻击。

美国网络战争准备已到最后阶段。近日，国家计算机网络应急技术处理协调中心日前发布《2018 年我国互联网网络安全态势综述》的数据显示，来自美国的网络攻击数量最多，且呈愈演愈烈之势。目前美国已经完成了从力量建设、法律制定、情报收集、攻击通道、网络结盟、实战检验等发动网络战争的全部准备，事实上成为人类社会最大网络威胁。

表 2： 美国网络战争准备已到最后阶段

准备	内容
力量准备	从扩编 40 支到增编 133 支网络战部队，美军摸索成熟了网络攻防能力“拷贝”的有效模式，其示范效应正在加速全球网络空间军事化进程
法律准备	从指导《塔林手册》到推出《网络空间联合作战条令》，美军拟定规范了网络行动的基本套路，这在一定程度上可以说明，美国网络战争准备已经完成了最后一道“工序”。
情报准备	从“五眼联盟”到“网络威胁情报整合中心”，美国形成了网络战争的决策能力，这一切足以说明，美国已经实质性具有了实施网络战争的决策能力。
通道准备	从设置“棱镜门”到入侵手机“芯片”，美国留下了无数发动网络攻击的便捷通道。
结盟准备	从进行“多国演练”到促进“共同防御”，结盟是美国发动网络战争的基本方式。美国的“网络结盟”运动基本上可以划分为三个交错演进的阶段：国内联合演习阶段、国际联合演习阶段、双边和多边网络攻防合作阶段。
实践准备	从伊朗“震网”到朝鲜“断网”，美军或由网络威慑走向网络行动。

资料来源：公开资料整理，东兴证券研究所

中美贸易战背后是科技战，同时科技战与网络战叠加共振。以华为事件为例，一方面，早在十年前，美国国家安全局（NSA）就开展了代号为“狙击巨人”的入侵行动，对华为总部网络实施了长达 7 年的攻击和监控，通过入侵华为内部邮件系统，掌握了包括任正非在内的华为高管的大量机密信息。另一方面，美国妄图谋取 5G 时代的网络数据权，“棱镜门”事件表明它一直在监听全球互联网。如果未来全球网络采用了华为 5G 技术和设备，美国想截获、监听它国数据就不那么容易了，打压华为成为美国政府的必然选择。

1.3 网络战随时爆发，中国应对策略迫在眉睫

据国家计算机网络应急技术处理协调中心日前发布《2018 年我国互联网网络安全态势综述》。数据显示，来自美国的网络攻击数量最多，且呈愈演愈烈之势。2018 年位于美国的 1.4 万余台木马或僵尸网络控制服务器，控制了中国境内 334 万余台主机，控制服务器数量较 2017 年增长 90.8%。在网站木马方面，2018 年位于美国的 3325 个 IP 地址向中国境内 3607 个网站植入木马，向中国境内网站植入木马的美国 IP 地址数量较 2017 年增长 43%。根据对控制中国境内主机数量及控制中国境内遭植入木马的网站数量统计，在境外攻击来源地排名中，美国独占鳌头 。

网络战已成为大国博弈的重要手段，加强网络战应对刻不容缓。近日，针对美国部署网络战，360 提出五大应对策略，包括转变防御思想，建设网络空间雷达反导系统，开展实网攻防演练，尽快攻克我国数字证书体系、DNS 等一批“卡脖子”工程。

打造国家级别的安全大脑。要明确指导思想。没有攻不破的网络，不要幻想马其诺防线。随着 5G 通信、人工智能、万物互联这一波技术革命的到来，未来的世界“万物均要互联、一切皆可编程”。要统一安全大数据。打造国家级的安全大脑迫在眉睫。网络战拼的不是武力值，最重要的是要看见攻击，要靠安全专家。网络攻防本质是人和人的对抗、战争，其中利用新技术来提升对抗效率是未来网络安全的发展趋势。当前时点，网络安全攻防还是高水平黑客之间的紫金对决，但更长期来看，新技术的应用，新业态的出现将是未来网络安全的主流。

2. 申威——保障党政军安全的“美国政府认证”产品

美国商务部当地时间 21 日以国家安全关切为由，将中科曙光(603019)和江南计算技术研究所等 5 家中国实体列入出口管制“实体清单”，禁止它们从美国供应商采购零部件。相关决定于 6 月 24 日生效。

这是继将华为公司列入“实体清单”后，美国对中国企业采取的又一起单边制裁行动。此次被列入“实体清单”的中国企业，主要业务与开发超级计算机有关。其中江南计算技术研究所在超算领域已经有自主技术的 CPU 申威。

申威核心业务包括申威处理器芯片内核、封装设计、技术支持服务及销售，小型超级计算机研发、测试、销售、服务及核心部件生产，基于申威处理器的软件、中间件开发，嵌入式计算机系统定制化产品服务，集成电路 IP 核等知识产权授权。

2.1 申威系列 CPU 性能卓越，覆盖面广

申威系列的主流通用 CPU 处理器，从单核、双核、四核、16 核，一直到比最新得 Intel 得中核处理器 Xeon Phi 7120P 性能更强得 SW26010 众核 CPU，种类齐全，性能卓越。

表 3： 申威系列 CPU 产品

类型	产品	内容
高性能单核处理器	SW111	高密度计算型嵌入式应用需求
	SW121	信号处理、网络安全、工业控制和嵌入式控制等领域应用
高性能多核处理器	SW221	面向高密度计算型嵌入式应用需求
	SW411	现已批量应用在网络安全、安全存储、高端工业控制、国产办公桌面等领域产品中
	SW421	面向中低端服务器和高端桌面计算机应用
	SW421M	面向中低端桌面计算机应用
	SW1621	面向高性能计算和中高端服务器应用。目前，该处理器已经实现量产
申威国产 IO 套片	SW-ICH2	申威 ICH2 国产 I/O 套片是在第一代 ICH1 的基础上，对产品安全适应性进行升级，增加外设启闭管控、数据通路密码保护等安全功能，实现 I/O 外设接口的高安全、防泄密和可管控要求
	SW-ICH1	申威 ICH1 国产 I/O 套片是一款完全自主设计的系统芯片，可与申威处理器或其他主流处理器配套使用

资料来源：公开资料整理，东兴证券研究所

申威系列主流的 CPU 产品，从制程工艺和技术水平上主要有 40nm 和 28nm 两种，SW121/SW411/SW1610 是使用了 40nm 工艺的单核、4 核和 16 核 CPU 处理器；而 SW221/SW421/SW421M/SW1621/SW26010 分别是使用了 28nm 工艺的 2 核、4 核、16 核以及众核（260 核）的 CPU 处理器。

从应用上分类，在分别搭载申威系列自主研制的 I/O 套片 ICH1 和 ICH2 的基础上，SW121 单核 CPU 主要应用于物联网、嵌入式工控机设备；SW221 双核 CPU 主要应用于物联网、嵌入式设备、个人(PAD)终端、笔记本电脑、专用电脑等领域；SW411/SW421/SW421M 等 4 核 CPU 主要应用于嵌入式工控设备、桌面电脑、笔记本电脑、低端服务器、网络设备等领域；SW1610/SW1621 等 16 核 CPU 主要应用于各种高端服务器、高性能网络设备、低性能超算等领域；SW26010 众核 CPU 主要应用于桌面高性能超算，大型、巨型超算领域 。

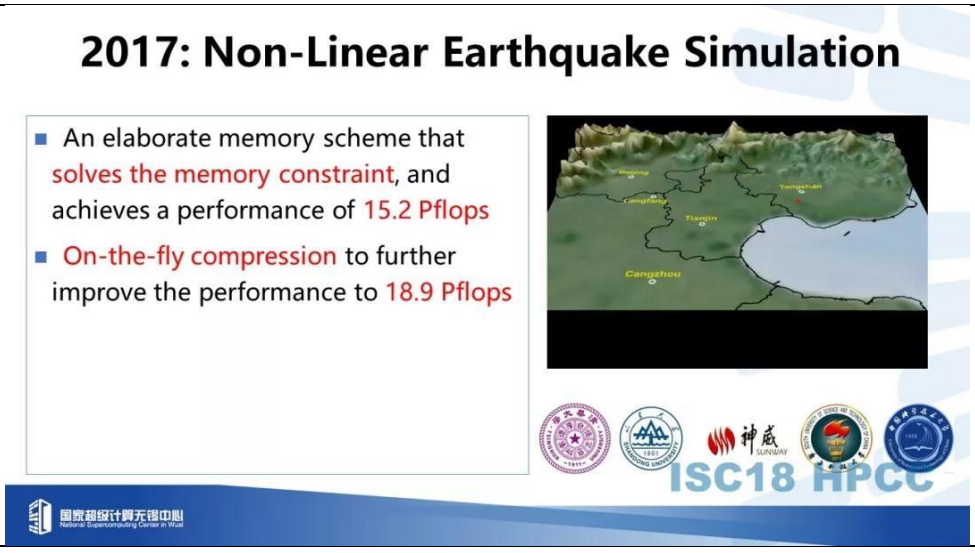
此外，中国曾霸占世界第一位置多年得神威·太湖之光超级计算机，所使用得处理器便为申威提供的。“神威·太湖之光”超算使用了 40960 个 SW26010 作为计算节点。正是得益于国产众核芯片 SW26010 的

强悍性能，加上良好的体系结构设计以及互联网络等核心部件，使该超算拥有异乎寻常的高性能、高效率、低功耗、高性能功耗比和小体积：

- 高性能--“神威·太湖之光”双精浮点峰值高达 125PFlops，稳定性能为 93PFlops，稳定性能是美国超算泰坦的 5.2 倍。
- 高效率--“神威·太湖之光”整机效率高达 74.16%，在稳定性能是美国超算泰坦 5.2 倍的情况下，整机效率依然大幅优于泰坦。
- 低功耗--“神威·太湖之光”的功耗为 15.3 MW，在稳定性能达到天河 2 号 3 倍的水平，但整机功耗却低于天河 2 号。
- 性能功耗比高--“神威·太湖之光”的性能功耗比高达 6G/W，即便是全球 Green500 排行榜，“神威·太湖之光”也能排至第三位。
- 小体积--“神威·太湖之光”机柜占地 605 平方米，美国超算泰坦机柜占地面积 404 平方米，天河 2 号机柜占地面积 720 平方米。
- 高可用性--在 2016 年、2017 年连续两年夺得“戈登贝尔”奖，且在近年来的应用越来越多。

2018 年，清华大学付昊桓教授提出了《基于“神威·太湖之光”的非线性地震模拟》的观点。清华大学林恒博士提出了一个超大规模图计算系统“神图”：它能够利用数百万个超级计算机内核，在半分钟内处理有多达 70 万亿条边的图数据。此外，申威·太湖之光还将被应用于机器学习进行高分辨率的图像土地分类，开发地球系统模式核航天飞行器统一算法数值模拟等。

图 2：基于太湖之光的非线性地震模拟



资料来源：公司官网，东兴证券研究所

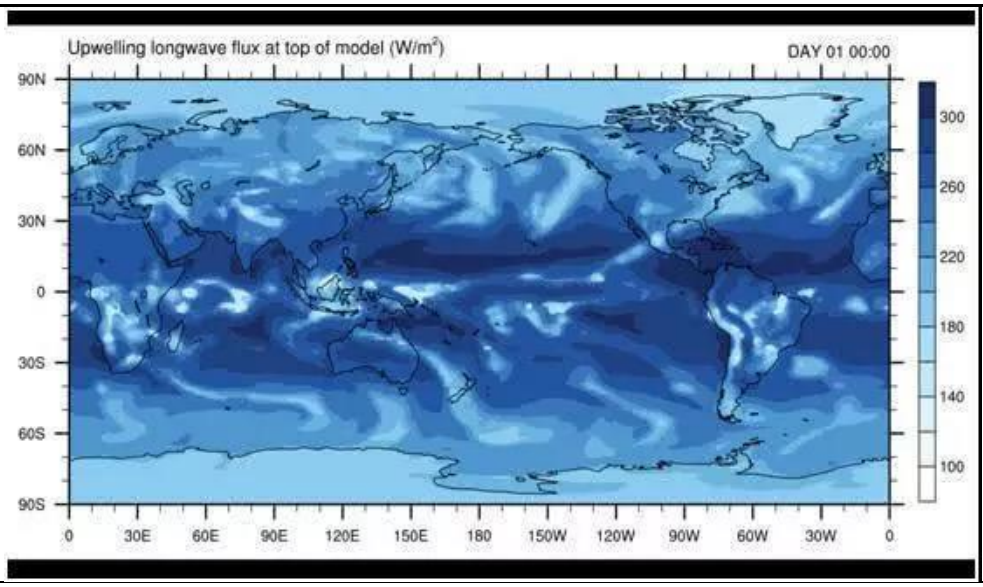
图 2：基于太湖之光的图像处理应用

资料来源：公司官网，东兴证券研究所

图 3：高分辨率的图像土地分类

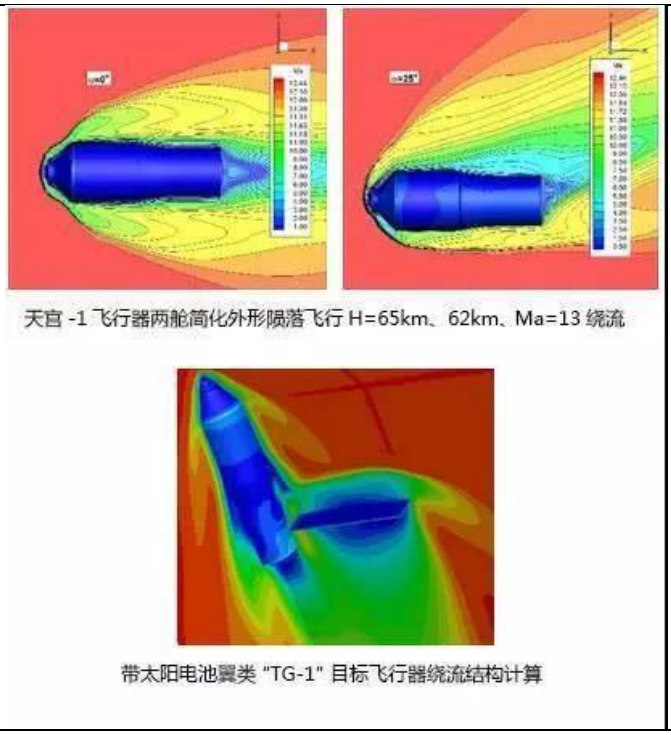
资料来源：公司官网，东兴证券研究所

图 4：基于国产平台的国产地球系统模式



资料来源：公司官网，东兴证券研究所

图 5：航天飞行器统一算法数值模拟



资料来源：公司官网，东兴证券研究所

因此，申威系列 CPU 不仅性能卓越，而且覆盖了几乎所有的通用 CPU 应用领域，随着使用申威芯片的不断发展和用户逐渐增多，必将为我国的科技新基建事业做出其应有的贡献。

2.2 申威生态链持续发展，产品技术日益丰富

申威 CPU 芯片的发展由于得到了军方的重点保障，一直按部就班、发展比较平稳，经过长期稳定的研发，基于系列申威芯片的各种产品也逐渐增多，在保障军方应用和国家战略任务的前提下，随着其产品技术的日益成熟，开始走向社会。

在国家军民融合政策的指导下，曾经得到军方应用支持的各种申威整机产品也能够走向党政办公市场，这些产品能够基本满足各种应用需求，包括办公桌面系统、服务器、网络设备、网络信息安全应用等。同时，申威 CPU 的各种开发支撑系统也已经非常成熟完善了，使得基于民用市场的产品开发也会愈加容易，开发周期也会大大缩短，越来越多的国内产品研发企业也能快速融入到申威生态链中。

表 4： 申威生态链

类型	产品	内容
申威 CPU 系列整机产品	单核 CPU 的嵌入式产品应用	
	双核、四核 CPU 的桌面终端核笔记本、以及低端服务器应用	S40 申威笔记本电脑（14 寸，申威 SW411 架构）； S40 申威加固笔记本（14 寸，申威 SW411 架构，抗震动，耐冲击）； S41-32A 一体机电脑（32 寸，申威 SW411 架构，带光驱）；
	16 核 CPU 的高端服务器、网络设备应用	基于 SW1621 的神威通用高性能服务器，如 ThinkSystemSR359S、飞龙 RS6012； 基于 SW1621 的神威 NAS 服务器； 基于 SW1621 的”中科神威“系列安全产品；
	众核 CPU 的桌面超算应用	第一代桌面超算产品使用众核处理器 SSW26010，第二代桌面超算产品使用上海国家高性能集成电路中心设计的申威二代众核处理器，运算能力于”神威·蓝光“相当；
申威 CPU 的开发配套软件	申威系列芯片的开发板核开发系统	基于 SW111 嵌入式系统开发板； 申威 SW411 系统开发板； 申威 SW421 系统开发板； 申威 SW412M/221 系统开发板；
	申威系列芯片的 BIOS	国产 BIOS 固件，支持身为芯片的主要有昆仑固件等；
	支持申威芯片的国产操作系统	中标麒麟桌面操作系统，中标麒麟服务器操作系统（申威版），深度操作系统（申威）桌面版，深度操作系统（申威）服务器版，嵌入式操作系统（申威版）
	支持申威系列芯片的虚拟机管理器	采用低开销虚拟化技术
	其他方面	基于申威芯片的 JAVA 移植优化方面、申威芯片的编译器等；
申威 CPU 的应用支撑系统	中间件	东方通是领先的新一代软件基础设施和创新应用提供商，处于中间件产品的行业领先地位，与各厂商形成完整的安全可靠解决方案； 金蝶天燕是国家规划布局内重点软件企业，数字化基础设施运营服务的开拓者和领航者；
	数据库	人大金仓与飞腾、申威等 CPU 和麒麟等国产 OS 深度适配优化，具备高安全、高可用、高扩展等使用特性； 作为国产数据库的领军企业，南大通用打造了 GBase 8a/8t/8m/8s/8d/UP 等多款国内领先的安全数据库、大数据产品； 武汉达梦是国家规划布局内重点软件企业，首批获得国家“双软”认证的高新技术企业，唯一获得国家自主原创产品认证的数据库企业，拥有国内顶级的数据库研发

	精英团队，多次与国际数据库巨头同台竞技并夺标；
申威的 CPU 的系列整机典型配套应用软件	目前常用的办公套件有中标普华、永中 office、(金山 WPS)；浏览器软件有 Firefox，Chrome；开发环境有 Eclipse、Qt Creator

资料来源：公开资料整理，东兴证券研究所

申威 CPU 处理器的国产化产业链布局完整，软硬件产品可堪重用，在国家“”863 计划”、“核高基”重大专项等项目的支持以及产业界持续的努力下,形成了以自主研发的申威 CPU 处理器为核心，中标麒麟、深度等操作系统厂商，以及南大通用、武汉达梦等数据库厂商为代表的国产安全产业体系。经过十余年的发展,国产安全核心产品与部件实现了从无到有的跨越,并通过国家重点项目以及军队的应用,申威通用安全类产品体系经过系统适配与优化后逐步从“基本可用”走向“基本好用”，已经具备了在政府、军队、央企等对网络安全有迫切需求的领域进行规模化推广的基础。

2.3 不受知识产权所限，完全自主

在我国自主信息技术发展的具体实践中，独立自主路线和技术引进路线处于并行状态。申威采用引进、消化、吸收、自主研制的技术路线，完全没有知识产权问题。

表 5： 国内几种 CPU 芯片的知识路线

芯片	申威	龙芯	飞腾	兆芯	海光	宏芯	华芯通	SOC
研制单位	上海高性能	龙芯中科	国防科大	上海兆芯	天津海光	中晟宏芯	美国高通	华为海思
指令集架构	ALPHA	MIPS	ARM	X86	AMD	POWER	美国高通	ARM
架构来源	自研	永久授权	期限授权	期限授权	期限授权	期限授权	贵州合资	期限授权
授权权利人	中国自主	英 Imagination	日本软银	Intel	AMD	IBM	美国高通	日本软银

资料来源：公开资料整理，东兴证券研究所

申威采用了 ALPHA 的指令集架构，完全自主研制了所有的指令集，达到了几乎完全的自主研制。

3. 互联网监管发展历程

3.1 我国互联网监管体系的历史变迁

建国以来，我国政府历来认为媒介的有效监管与整个国家的治理和发展紧密相联，在互联网领域，由于其功能的多元化，以及政府在不同时期对互联网重视 领域的不同，使得我国互联网监管的历程呈现如下变迁轨迹。

第一阶段，互联网监管的空白时期（1987-1993 年）：以科研机构自治为主

这段时间，政府基本没有介入互联网的监管，零散出现的互联网问题，主要由使用单位科研机构自身来解决。

第二阶段，互联网监管的起步时期(1994-1997 年)：侧重于主干网搭建、域名管理、IP 地址分配等基础设施的扶持

1994 年，我国正式接入国际互联网，但此时由于互联网基础设施建设刚起步，很多领域都处于“零基础”或“低水平”状态， 因此，在互联网的治理方面，我国政府将主要精力投入到了主干网搭建、域名管理、IP 地址分配等促使互联网正常运转的基础设施的治理上。

第三阶段，互联网监管的体系化时期（1998-2004 年）：采取“ 先发展，后管理”的宽松监管理念

当互联网运用逐步广泛进入社会领域时，我国对互联网的监管不再仅局限于对互联网基础设施的治理，而且也延伸至对互联网内容、信息服务等领域，初步搭建 了一整套监管体系。

第四阶段，互联网监管的现代化时期（2005 年-至今）：强调互联网自治规律

当我国进入互联网 WEB2.0 时代后，面对全新的信息传播格局，我国既有的以传统媒体的监管体系为主要参照 的互联网监管体系明显不足。因此，应摸清并遵循互联网传播的自身规律，促使现有互联网监管的现代化，进而建立现代科学的互联网监管体系。

3.2 互联网监管的新的政策要求

等级保护进入 2.0 时代，网络安全保护政策、标准和支撑体系不断完善。2019 年 5 月 13 号，《信息安全技术网络信息安全等级保护基本要求》国家标准正式发布,新标准将于 2019 年 12 月 1 日正式实施，标志着我国网络安全等级保护工作正式进入“2.0 时代”。相较于 2007 年实施的《信息安全等级保护管理办法》所确立的等级保护 1.0 体系，等级保护力度从条例法规提升到法律层面，在标准名称、保护对象、章节结构、控制措施等多个方面进行了更新与完善，更注重全方面主动、动态防御和精准防护。

图 6：网络安全等级保护 2.0 体系构架

资料来源：公司官网，东兴证券研究所

我国需推动和加强社交网络平台安全监管。社交网络平台改变了传统信息传播的固有模式，它能在短时间内将信息从一点辐射全球，超越了领土边界的固有限制，跨越了政治、民生、经济等多个领域。在今年 5 月 28 日中央网信办发布的《数据安全管理办法（征求意见稿）》中，其第二十五条针对用户转发对社交网络平台提出了新的要求。网络运营者应建立相关机制，要求用户对自己发布的信息负责，用户则应在发布信息前对信息内容的真实性和影响等进行确认和考虑，尤其是对转发信息要慎重。我国国家互联网信息办公室先后发布了《即时通信工具公众信息服务发展管理暂行规定》、《互联网用户公众账号信息服务管理规定》等规定，要求服务提供者落实主体责任，建立健全安全管理制度，要求用户通过真实身份信息认证后注册账号，加强对其用户发布信息的管理等。

4. 科技新基建

4.1 我国科技新基建信息技术实施情况

目前国产科技新基建路径上，主要包含三大类，第一、突破式，包括北斗导航，云计算、电子信息技术等；第二、加速式，包括大飞机，医疗器械等；第三、起步式，包括芯片，创新药仿制药，网络安全，人工智能等。

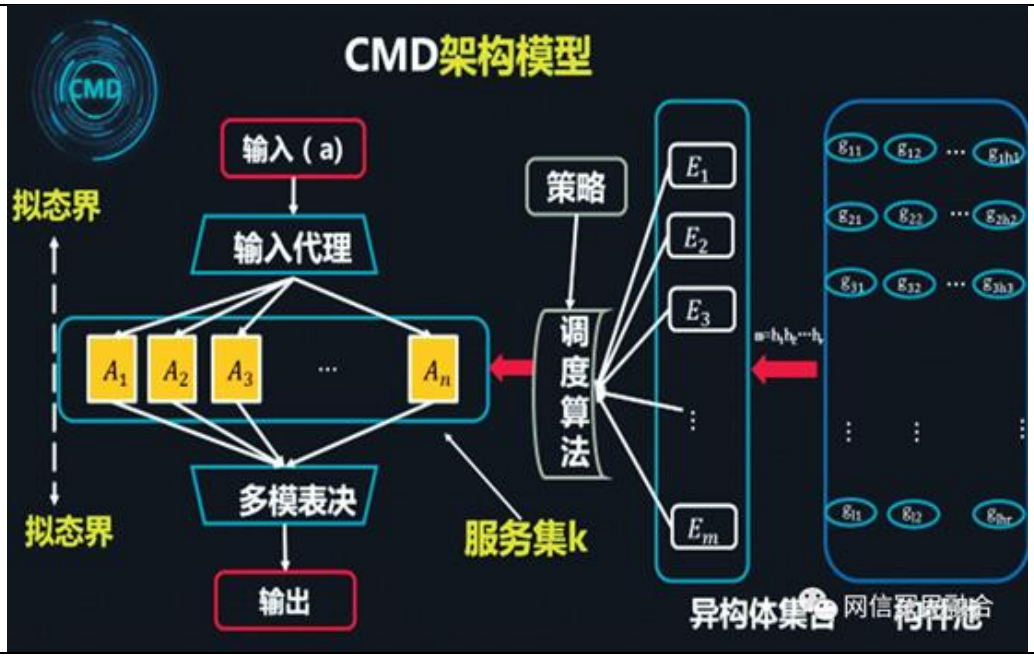
4.2 拟态防御

中国网安挑战赛夺奖，拟态防御带来网络安全新机遇。近日，第二届“强网”拟态防御国际精英挑战赛在南京江宁圆满落幕。中国网安旗下三零卫士广州公司派出的木星安全实验室代表队受邀参加此次比赛，在与十国精英的角逐之中成功斩获大赛“优胜奖”，展现了团队的优良实力。

拟态防御技术理论是邬江兴院士研究团队首创的主动防御理论，可为应对网络空间中不同领域相关应用层次上基于未知漏洞、后门、病毒或木马等未知威胁，提供具有普适创新意义的防御理论和方法。目前，拟态防御已在军事领域有所应用，最为典型的是隐形飞行器或舰船。

网络空间拟态防御的愿景是，能够应对拟态界内未知漏洞后门等导致的未知风险或不确定威胁；拟态防御的有效性由架构内生防御机制决定而不是依赖现有的防御手段或方法；不以拟态界内软硬构件的“可信可控”为前提，适应全球化开放生态环境；能够融合现有的任何安全防护技术并可以获得超非线性的放大防御效果。期望解决基于不可信供应链构建“安全可信”系统的“网络时代经济学”难题；最大程度降低攻击者经验的可复现性和传播价值；显著提高攻击者入侵难度和获利代价，逆转“易攻难守”格局。最终寻求“构造决定内生安全”的革命性防御能力。

图 7：网络空间拟态防御模型



资料来源：公司官网，东兴证券研究所

拟态防御的有效性虽然在理论上已经得到证明，但工程实践效果如何仍需要严格的测试验证和分析评估。并且，尽管拟态防御基本原理与方法具有普适性，但是不同领域可能面临不同的应用挑战，理论和技术层面尚需不断完善与再创新。

4.3 政策支持

表 6：相关政策全景

时间	政策
1994 年	《中华人民共和国计算机信息系统安全保护条例》
1997 年	《计算机信息系统安全专用产品检测和销售许可证管理办法》
2003 年	《国家信息化领导小组关于加强信息安全保障工作的意见》
2006 年	《我国信息产业拥有自主知识产权的关键技术和重要产品目录
2007 年	《信息安全等级保护管理办法》
2010 年	《关于信息安全产品实施政府采购的通知》
2010 年	《中华人民共和国保守国家秘密法》
2011 年	《进一步鼓励软件产业和集成电路产业发展的若干政策》
2012 年	《“十二五”国家战略性新兴产业发展规划》
2014 年	《中央国家机关政府采购中心重要通知》
2014 年	《国家集成电路产业发展推进纲要》
2014 年	《加强电信和互联网行业网络安全工作的指导意见》
2015 年	《国家安全法》
2015 年	《国务院关于积极推进“互联网+”行动的指导意见》
2016 年	《国家网络空间安全战略》发布
2016 年	《关于印发国家规划布局内重点软件和集成电路设计领域的通知》
2016 年	《国家信息化发展战略纲要》
2016 年	《“十三五”国家信息化规划》
2017 年	《软件和信息技术服务业发展规划(2016—2020 年)》
2017 年	《网络安全法》
2018 年	《深化党和国家机构改革方案》
2018 年	《关于推动资本市场服务网络强国建设的指导意见》
2018 年	《关于集成电路生产企业有关企业所得税政策问题的通知》

资料来源：东兴证券研究所

技术安全管理清单将出。根据《国家安全法》等相关法律法规，国家发展改革委正牵头组织研究建立国家技术安全管理清单制度，以更有效预防和化解国家安全风险。具体措施将于近期出台。从长远看，针对我国优势核心技术，建立国家技术安全管理清单制度，也将为我国实现创新驱动、走高质量发展之路奠定更加坚实的制度基础。

应用试点示范项目推出，网络安全技术将于各领域推广。2018 年底，国家工业和信息化部为深入贯彻落实《中华人民共和国网络安全法》，加快建设网络强国，促进信息安全行业发展，决定开展网络安全技术应用试点示范项目推荐工作。此次入选的 101 个项目中，均已投入运营，且与实际应用场景深度结合，具备高度的实用性、创新性和可推广性，将在各核心领域进行持续应用推广。

5. 风险提示

等保 2.0 落地速度不及预期，网络安全行业发展不及预期，国产安全业务发展不达预期。

表 7：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

相关报告汇总

报告类型	标题	日期
行业	【东兴军工】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	2019-05-14
行业	安全可靠工程半月谈之二：科技战本质是网络战，网安携“乌媒”布局互联网监管	2019-05-27
公司	【东兴军工】卫士通（002268）事件点评：中国网安以电科信链发力政务区块链	2019-05-08
公司	中国长城（000066.SZ）深度报告系列之四：自主可控将加速推进，从党政军扩展至重点行业	2019-04-15

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。