



点融秋季安全沙龙

战略角度看安全：

金融科技信息安全的 黑暗森林法则



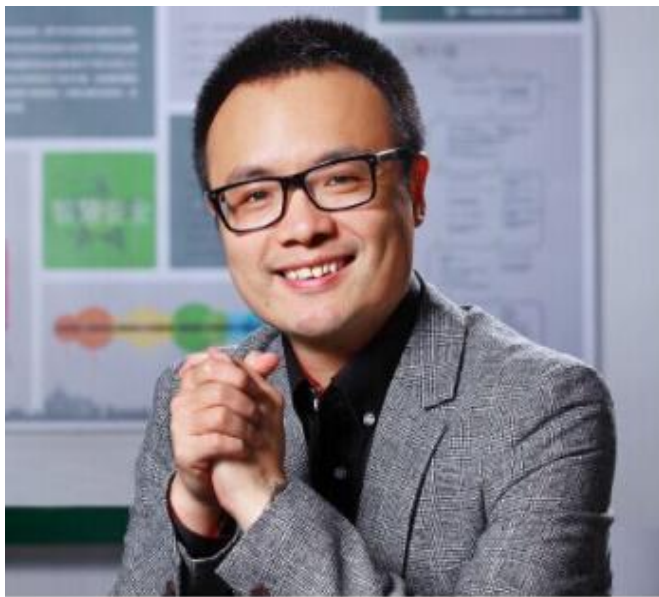
青藤云安全

郝东林

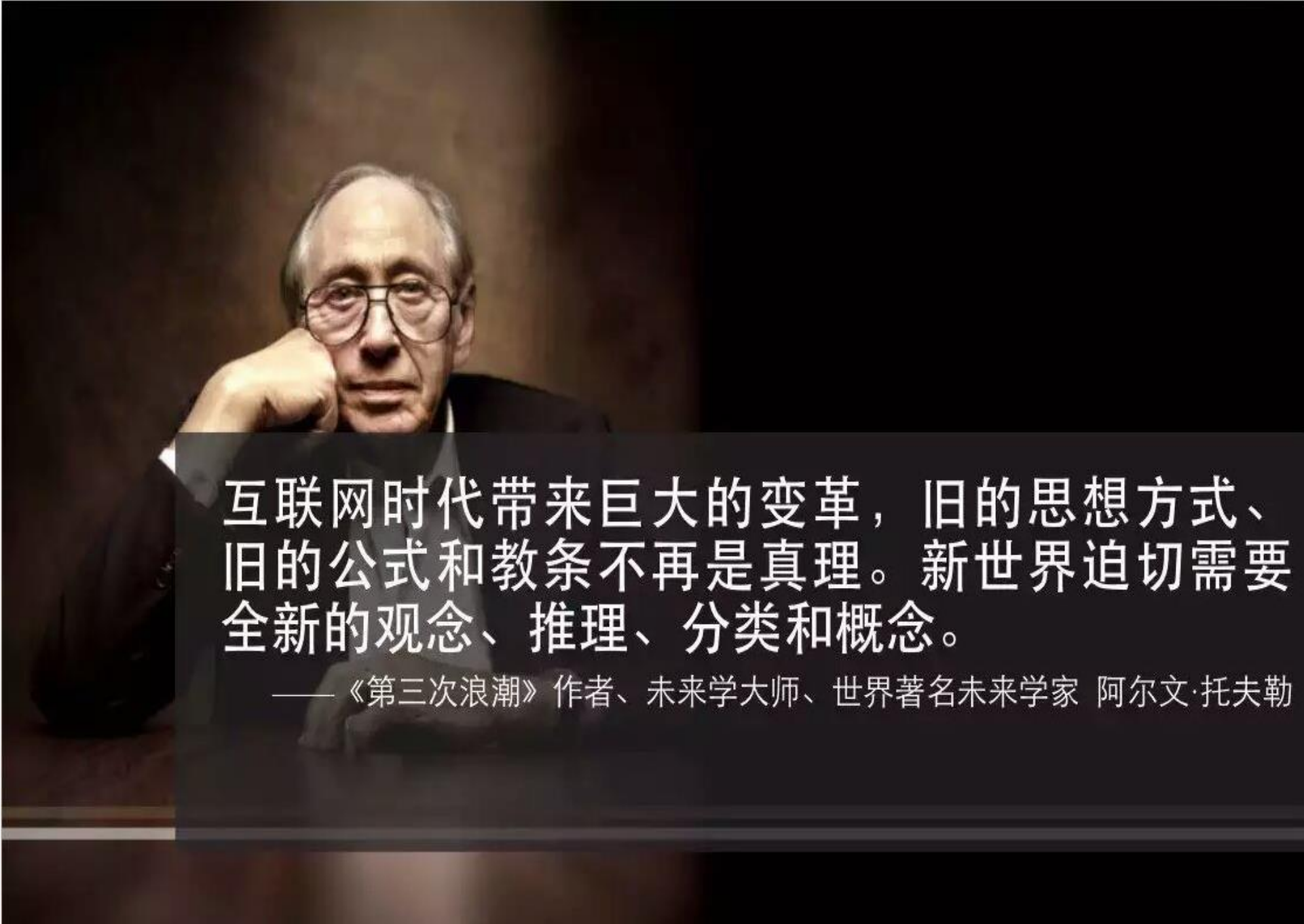
2016.10.30 上海



个人介绍



- 郝东林，现任青藤云安全合伙人&副总裁。清华大学五道口金融学院未央网、金融咨询网、百度名家专栏作家，国家开发银行专家库成员，2014年度“中国金融科技企业杰出人物”，国际云安全联盟CSA STAR 云安全注册评估师，2016年“中国互联网金融年度新领军人物”。著有《互联网+：金融与信息安全的行业变革》，工信部《互联网金融风险控制》副主编。
- 近五年时间，与全国超过100家金融机构、20多个省份银监局、人民银行合作，做过超过100场专题信息安全意识培训工作，受众人数超过万人，并协助监管机构做了部分金融行业监管标准的制定工作。

A portrait of Alvin Toffler, an older man with glasses, resting his chin on his hand. The background is dark and moody.

互联网时代带来巨大的变革，旧的思想方式、
旧的公式和教条不再是真理。新世界迫切需要
全新的观念、推理、分类和概念。

——《第三次浪潮》作者、未来学大师、世界著名未来学家 阿尔文·托夫勒

这些年：我们知道的安全圈大牛



滴滴信息安全战略副总裁弓峰敏

弓峰敏博士被誉为硅谷安全创业教父，在网络及安全研发领域有着三十多年的经验，加盟滴滴之前是AssureSec联合创始人兼CEO，此外，弓峰敏博士是世界著名网络安全公司Palo Alto Networks的联合创始人，还是多家新兴安全公司的创始人或重要高管，其中三家企业已成功上市或被收购，他也是连续创业者和硅谷天使投资者。



滴滴信息安全副总裁卜峥

卜峥在信息安全企业有着丰富的从业经验，他在2000年联合创办绿盟科技，是国内最早从事网络安全的企业之一，并在美国三大安全软件企业之一的McAfee任威胁研究总监近十年，带领团队进行了世界范围内的信息安全研究，他和他的团队在入侵检测、恶意软件、高级威胁和威胁情报等方面都有着深入研究。加入滴滴之前他是AssureSec联合创始人兼总裁。

这些年：我们知道的安全圈大牛



百家——23岁贩毒，70岁竞选总统， ...

这位狂人就是我们今天要聊的吊炸天的老爷子——约翰·迈克菲（John McAfee）。

他的人生比任何电影都精彩100倍。

他贩毒、嗑药、酗酒、乱性、入狱，有“美国的韦小宝”之称。

他拥有数学博士学位，创办了全球著名杀毒软件McAfee，如今70岁的他要竞选美国总统。

在谷歌中搜索“网络安全传奇”，25万条搜索结果中，前10条的名字一定是迈克菲。

这位牛逼闪闪的人物出场画风一般是这样的



名词来源



名词解释：二向箔

名词来源：刘慈欣科幻小说《三体III：死神永生》。

事物属性：宇宙在黑暗森林状态下，星际文明的一种毁灭性攻击武器。

物理形态：一个被力场包裹的“小纸片”。

攻击原理：与三维空间接触的瞬间，使三维空间的一个维度蜷缩到微观，从而使三维空间及其中所有物质跌落到二维，使对方在三维宇宙中无法存在。

应对方法：空间跌落蔓延速度小于光速，因此只有以接近光速脱离的物体才可以避免伤害，其攻击范围最终据信会达到星系级别空间，甚至可能更大。

降维攻击与黑暗森林法则

宇宙社会学的基本公理：

- 1、生存是文明的第一需要；
- 2、文明不断增长和扩张,但宇宙中的物质总量保持不变；

高级公理：

- 3、猜疑链：一个文明无法判断另一个文明判断自己对她是善意或恶意的；
- 4、技术爆炸：文明进步的速度和加速度不见得是一致的，弱小的文明很可能在短时间内超越强大的文明。

大佬们的战略观点



全球市值排名前五
的都是互联网公司。

云端化
(SAAS化)

大数据化

智能化

降维攻击法则:互联网这个圈子好像有些人中了它的毒.....



- 1、A产品与B产品有着高度重合的用户。
- 2、A能实现B能做的所有事情，但B却不能反过来做A的主业务，并且A做的不错。
- 3、A将绕道式侵吞B的部分市场份额，甚至全吞。例如微信与中移动的短信业务关系。

案例分析

- 1、小米手机以及小米路由器将会是未来第一高维阵地，所以这两个关键产品永远必须需要亲自来做，而剩下的智能领域的低维战场则交给其他公司，如小米手环、小米插座等等，小米手机这一高维将会为其不断持续输血，构建一个庞大的森林体系，对所有没有高维支撑的厂商展开杀戮，小米的估值不在于手机而在于其降维攻击能力。
- 2、BAT都知道不能自己通吃一切，必须尽量抢占更高维度，排兵布阵，自己做不了的交给别人来做，并且其中每一个布局都说不定有可能在未来成为某个领域的高维度，让对手无法下手。所以才有了各种井喷式的投资并购，京东、大众点评与腾讯，高德与阿里，糯米与百度等等系列。

维度分析

主干维度链条	流量产品——→利益相关者——→盈利产品			
节点属性维度	外观 功能 服务 体验 安全 价格 品牌 口碑 关联性	生理、心理 文化、习惯 认知 分享 行业 社会属性 资源能力 利益诉求 结合方式	外观 功能 服务 体验 效用 个性化 差异化 附加值 稀缺性	
过程衍生维度	商业关系 支付 物流 互联网金融	信息 大数据 咨询 广告	金融 供应链金融 金融衍生品	能力 行业延伸 跨界

互联网模式打败传统企业采取的方式基本是：拓展出**新**的维度，然后把跟传统企业相同的维度**免费或者平价化**，抢夺市场空间，并在**新**的维度上获得**新**价值。这就是用“多维”打击“少维”，也就是通常说的“降维攻击”：把竞争对手原有的维度赋值降为**零**。

巨头们随时可能被颠覆



VMware与宿敌Amazon一笑泯恩仇：重新定义混合云？

2016-10-11 Mona IT战略家

三年前，虚拟化巨头VMware曾对亚马逊Amazon云服务AWS竖过中指：我们怎么可能打不过卖书的？并严厉警告其合作伙伴：“如果我们的客户都用了AWS公有云，你们统统破产关门！”

AWS呵呵：“如果有人认为我们只是书贩子，那好极了！”

随后，VMware在一年一度的VMworld大会上公布了备受瞩目的vCloud Hybrid Service (以下简称vCHS) 混合云服务。而这一项服务的推出，意味着VMware已经走出单一的私有云市场，去拓展更大的开放性云市场；

今天，如果一家公司考虑采用公有云，几乎近100%会优先考虑亚马逊。甚至连AWS的竞争企业，也不得不承认：“AWS是一种动力，没有一家高科技公司可以忽视它所带来的价值”。AWS作为全球第一个向市场推出IaaS产品的最大公有云厂商，2015年收入近79亿美元，增速超过50%。

面对残酷的现状，VMware首席执行官Pat Gelsinger的反公有云反AWS立场开始软化，虽然打自己的脸不好受，但事实让VMware也不得不承认：公有云正在取得优势，而AWS已经成为公有云的绝对领导者。VMware不得不认识到：他们可能已经输给了卖书的。那么VMware还要不要和“书贩子”继续死磕？！一个代表私有云，一个公有云，两家科技巨头的争斗，这其实是私有云和公有云之间的竞争。

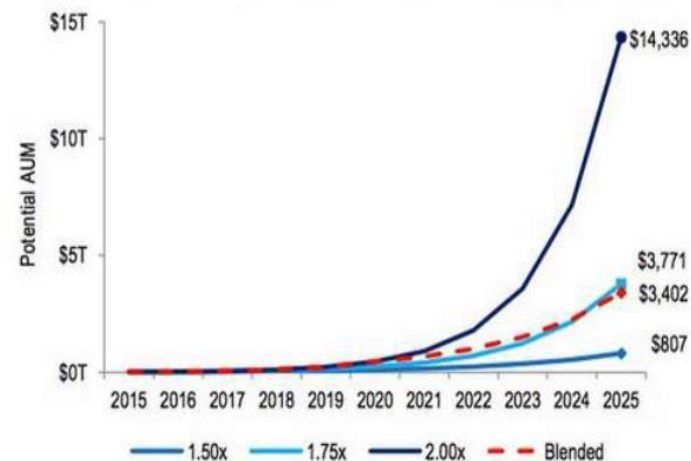
快技术

Blockchain as a Service (BaaS : 区块链即服务)

- 保证数据不可篡改
- 使得商品具有唯一可验证的身份，可鉴别真伪
- 透明的供应链管理
- 产业化智能合约

花旗集团曾有报告指出，机器人顾问所管理的资产从2012年零点，激增到2014年底的140亿美元。报告预测，在未来十年时间里，机器人顾问管理下的资产将会呈现出爆发增长的势头，有望达到5万亿美元。

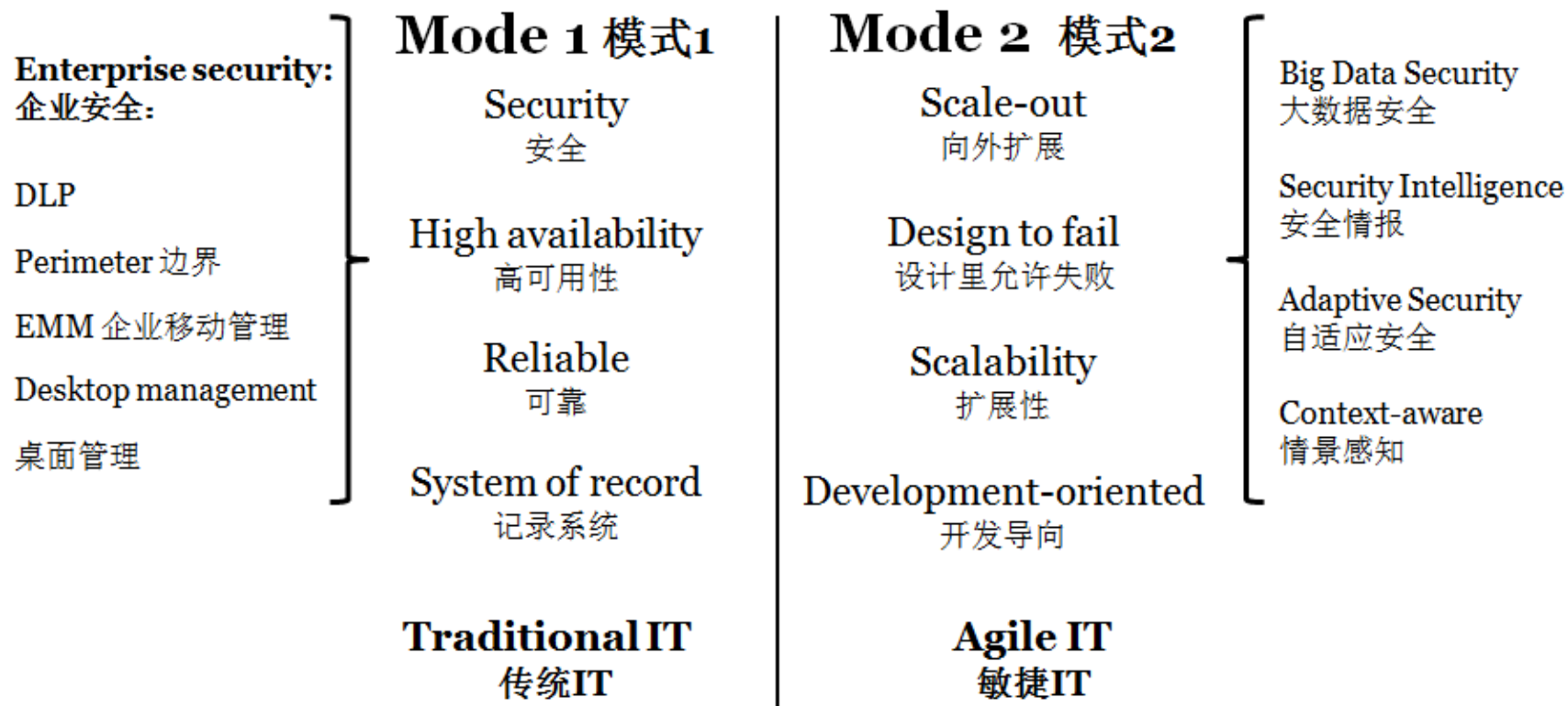
Figure 12. Potential growth trajectories for US Robo-advised AUM, starting at \$14B end-2014



机器人投顾红火的根本原因，便宜！

双模IT

Bi-modal IT 双模IT



WHY?

技术爆炸→速度为王



- 宇宙中的光速
- 人的理解和思维跟不上时代的发展
- 整个互联网发展的速度超过了大公司信息能够处理的速度

从三体分析人物关系与理论体系

《三体》游戏里出现的人物



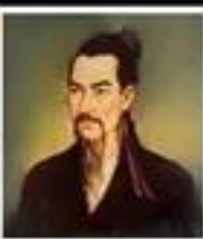
周文王



纣王



伏羲



墨子



孔子



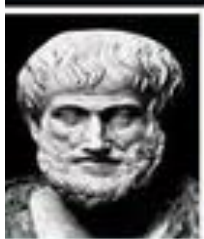
汉武帝



哥白尼



格里高利教皇



亚历士多德



伽利略



达·芬奇



布鲁诺



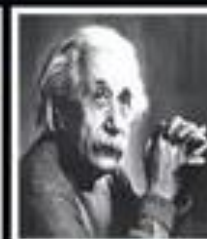
牛顿



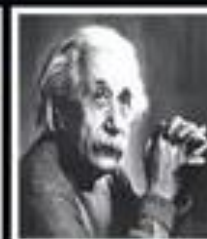
莱布尼茨



冯·诺伊曼



秦始皇



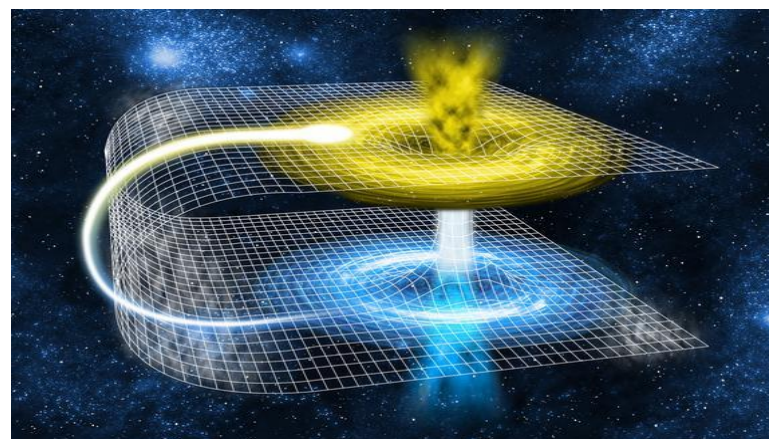
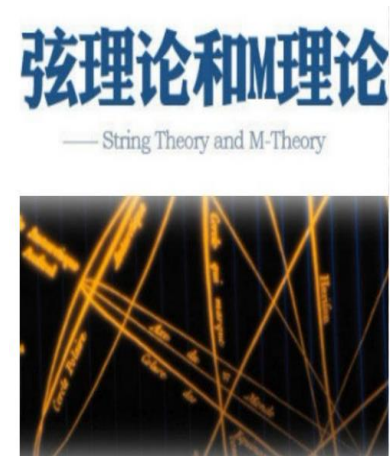
爱因斯坦

西方的哲学和物理学

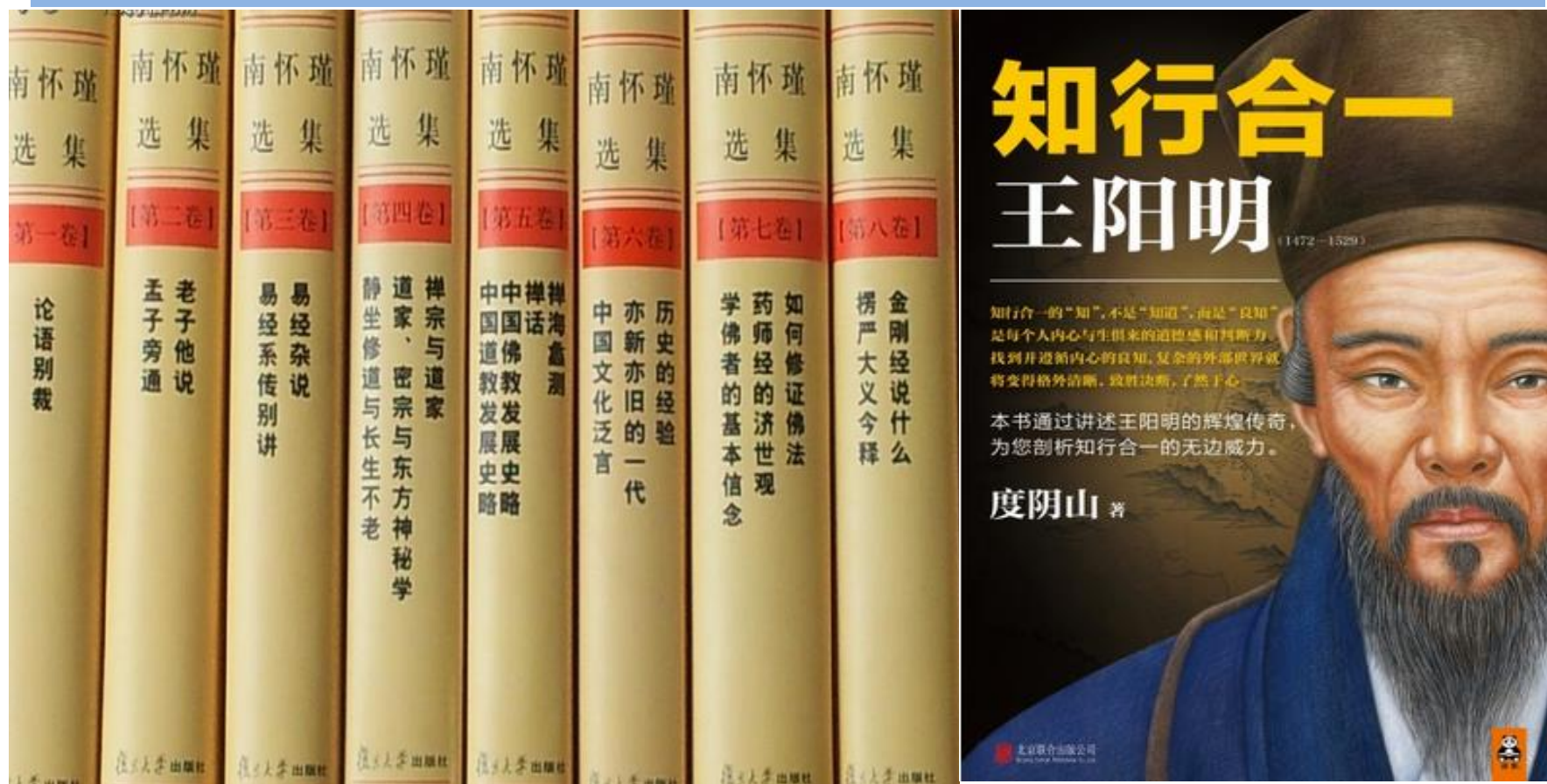
西方哲学研究

人的一生有三个阶段：

- 1、**前自我**：由胚胎到儿童，依赖他人获得成长；
- 2、**心智自我**：由青年到中年，人生所有的表象成就（名、权、利）都在这个阶段获得；
- 3、**超自我**：随着身体的衰落，心智自我渐渐破裂，开始超越个体的限制，与整个存在合为一体。



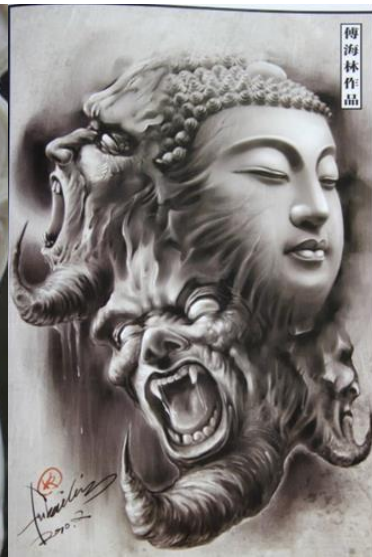
东方的国学



2011年5月，习近平视察贵州时，在贵州大学中国文化书院讲话时也谈及王阳明。他说他很景仰龙场悟道的王阳明先生，贵州的文化传播人对王阳明先生的学习，更应该有深刻的心得。我们的古代优秀文化值得自豪，要把文化变成一种内生的源泉动力，作为我们的营养，像古代圣贤那样格物穷理、知行合一、经世致用。

黑暗森林与人的思维的关系

**黑与白，攻与防；
善与恶，罪与罚。**



信息安全行业的黑暗森林法则

网络黑产规模破千亿，远超信息安全行业投资！

黑客攻击规模持续上升，金融、互联网金融、游戏、电商、直播是重灾区！

刷单、欺诈呈现专业化和产业化

网站入侵、拖库，数据无时无刻存在泄漏风险

APP假冒、钓鱼网站盛行

我悄悄的来了，入侵了你的主机，拿走了你的数据，又悄悄的走了。
挥一挥手，不留下一点痕迹.....

方院士对云计算与云安全的观点论述：猛兽与黑暗森林

	安全	可信	可靠	可控
基本假设	恶意假定	好人假定	老天假定	规则假定
类比	猛兽	宠物狗	牲畜	孩子
应用原则	监狱原则	办公室原则	猪圈原则	居家原则
出发点	事前保护	事后追责	经济平衡	了如指掌
应用点	未知身份	已知身份	随机因素	自有系统
追求目标	不受伤害	确是好人	不受损失	预料之中
手段	降低风险	依赖历史	投保机制	行为监控
风险	资源消耗	意外变节	概率损失	失控

信息安全行业的降维攻击法则

1、在移动端，安全问题已不是最高维阵地，因为就算杀毒软件掌控了底层系统，也无法掌控用户安装什么软件，用什么浏览器，用什么搜索引擎等等这种失控，也就导致了360无法再继续延续PC时代的优势，彻底失去了高维优势，其移动市场的搜索份额也自然非常低，因此老周又重新回去与酷派联合做手机，又专门成立了360企业安全集团的这个部门，如果对外进行商业化运营，很容易成为“高维度”公司，对其他公司进行“降维攻击”。

观点：
云计算时代的到来，信息安全行业的
降维攻击将会产生在哪里？

如果我是**滴滴**.....%¥#@！



信息安全圈的黑暗森林法则

成人世界的互联网

你眼中的“黑客”到底是谁？



世界上只有两种网站，一种是已经被黑的，另一种是正在被黑的。

一把沙漠之鹰价

值1450美金、一个伪造的英国护照价值

2000英镑、一克纯可

卡因价值80美金、一

张个人信用卡信息价

值14美金、黑入邮箱

的服务价值200美金，

而一个人的生命值

10000美金。

对黑暗森林不了解

企业安全现状与问题



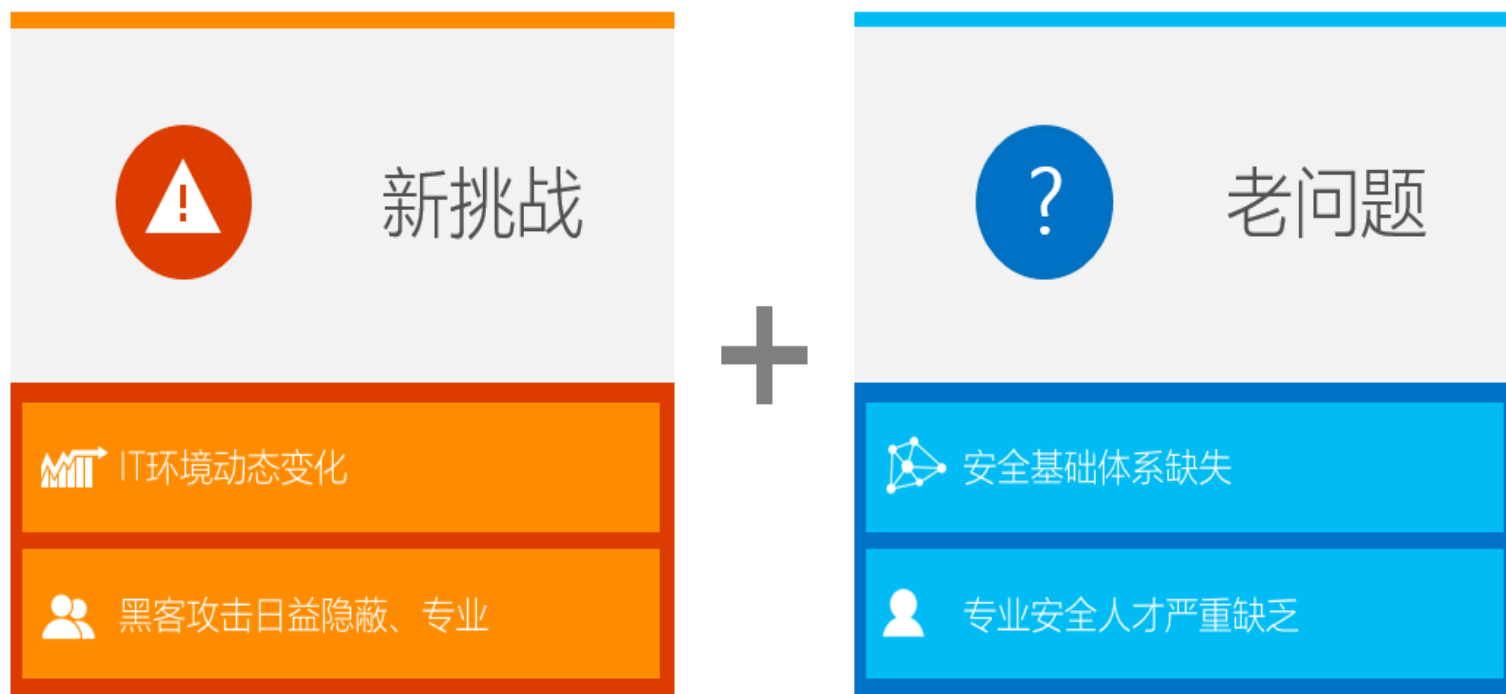
安全事件发生前



安全事件发生后

传统安全 VS 云安全

云时代的新挑战+老问题



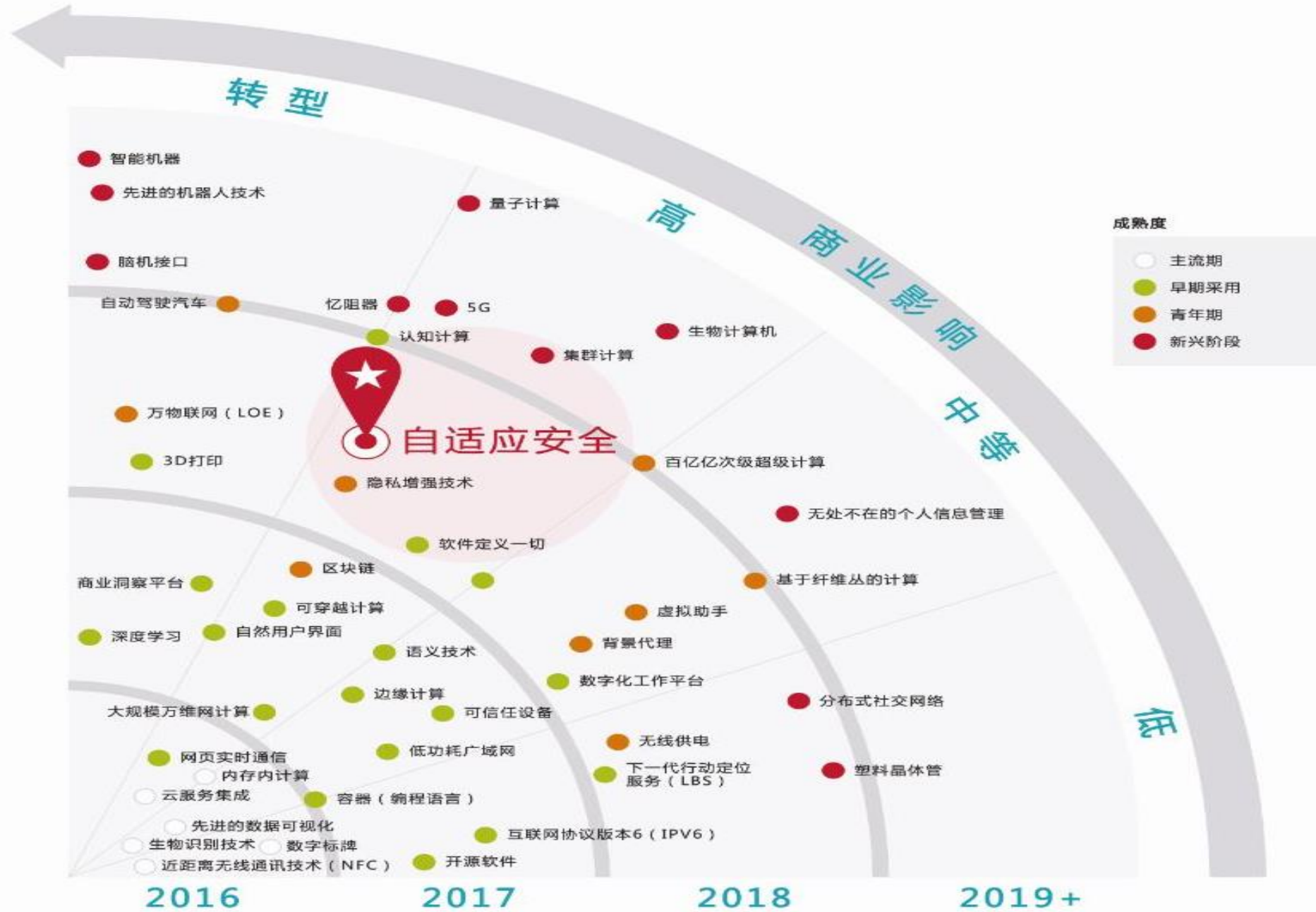
Gartner:自适应安全模型



传统安全 VS 云安全



更多区分，可以关注“青藤云安全”微信公众号或者今日头条APP“青藤号”，进行了解。



知行合一



信息安全部门的战略地位

信息安全意识培训

- 1、高管版；
- 2、中层业务部门管理版；
- 3、IT部门版；
- 4、全体员工版。



金融科技未来何去何从

行业维度

一、互联网+金融带来的颠覆与冲击，理论依据在哪里？（互联网界的“黑暗森林法则”：生存、扩张、猜疑链、技术爆炸）

二、两条出路：

a. 大者恒大。

b. 技术领先（业务创新）。

三、结论：

- 1、做大做强
- 2、细分领域王者
- 3、被并购
- 4、破产重组

技术维度

一、行业上云——大势所趋

二、安全问题——重中之重

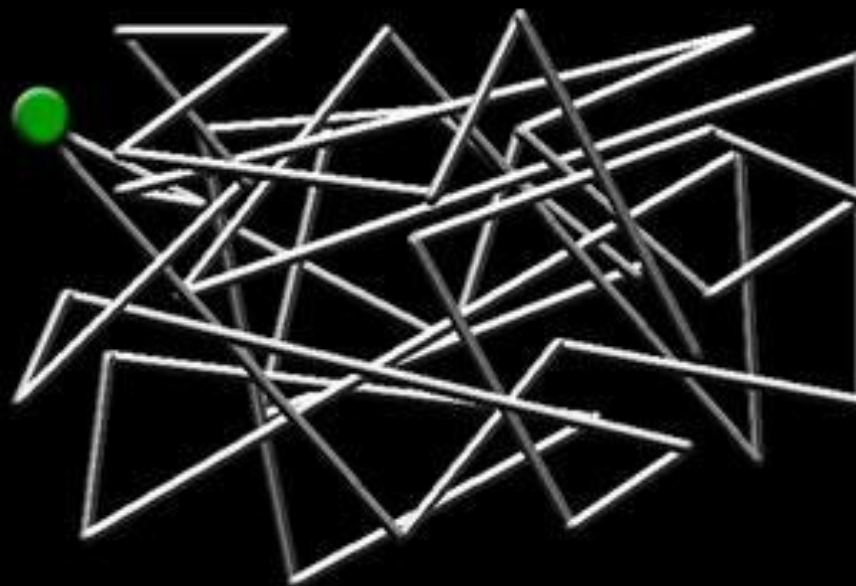
三、数据价值——最大资产

四、监管创新——迫在眉睫

不是你想象不出，有些事情就不存在.....



这是人在三维空间的样子



这是人在四维空间的样子

更多关于该问题的论述，参考微信公众号：“金融安全知行合一”

变革五部曲

- 1、坦然面对变革。
- 2、面对变革，从容进化。
- 3、找死——可能活的更好。
- 4、等死——必死！

金融科技安全实践分享



祝愿我们都能更好的活着！

THANKS



独角兽背后的安全专家
www.qingteng.cn



微信号：[hotonny](#)

主办单位： 点融网
Dianrong.com

协办单位： 青藤云安全



中国互联网金融企业家俱乐部
Entrepreneur Club of Internet Financial of China