腾讯全球数字生态大会
TENCENT GLOBAL DIGITAL ECOSYSTEM SUMMIT

Tencent 腾讯 | 腾讯安全 Tencent Security

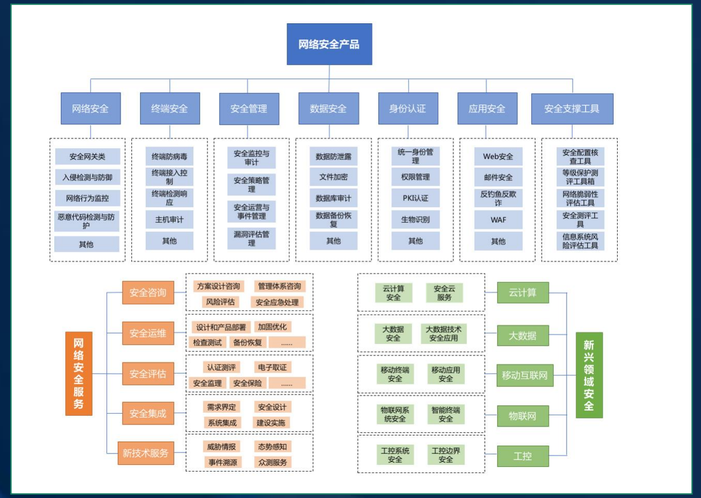
中国网络安全产业发展现状及展望

赛迪顾问软件与信息服务业研究中心总经理
高 丹

中国网络安全产业界定

➢ 网络安全是指包括涉及到互联网、电信网、广电网、物联网、计算机系统、通信系统、工业控制系统等在内的所有系统相关的设备安全、数据安全、行为安全及内容安全的产业。

中国网络安全产品生态图



- 网络安全产品是指保障网络系统安全的产品，可分为网络安全、终端安全、安全管理、数据安全、应用安全等。
- 网络安全服务是指保障网络安全分析评估、规划设计、认证测评、运维服务、咨询与培训等。
- 随着云计算、大数据等新兴技术的快速发展，网络安全应用领域日益广泛，软硬件产品的界限愈发模糊，产品和服务的联动更加紧密。

目录

现状一：安全防护监管日趋严格

2014年2月
中央网络安全与信息化领导小组成立

2016年4月
习总书记发表“4.19”讲话
2016年12月
《国家网络空间安全战略》发布

2017年6月1日
《网络安全法》正式施行
2017年
网信办及各部委发布《国家网络安全事件应急预案》、《关键信息基础设施安全保护条例〔征求意见稿〕》等

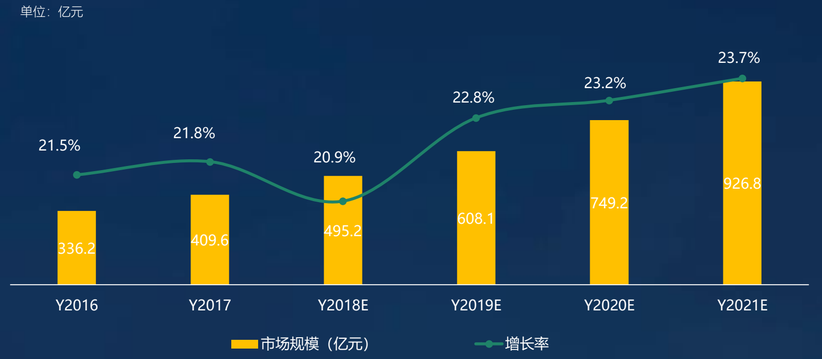
2018年6月
公安部发布《网络安全等级保护条例〔征求意见稿〕》

2019年5月，《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准正式发布，将于2019年12月1日开始实施

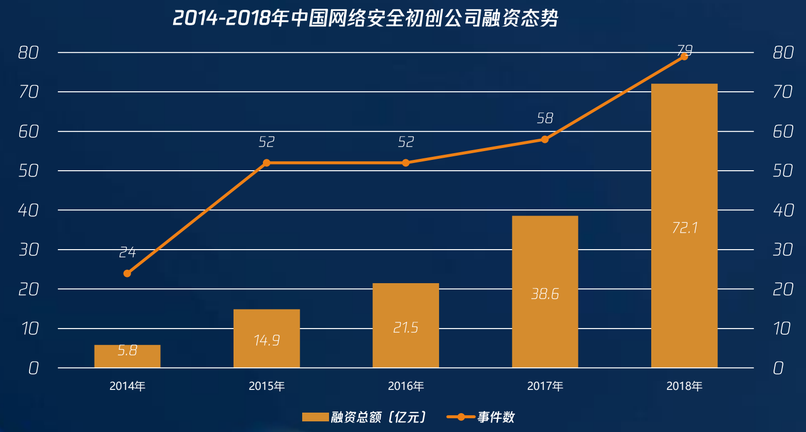
现状二：网络安全市场稳步增长

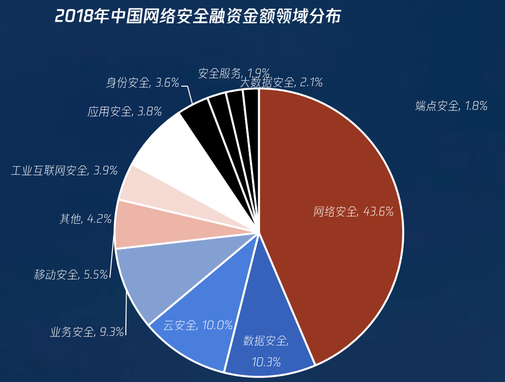
2016-2021年全球网络安全市场规模与增长

2016-2021年中国网络安全市场规模与增长



现状三：网络安全市场投融资持续火热





- 2018年，中国投融资金额和交易数量都大幅上涨，而单笔融资金额也不断上涨，亿级融资20起，千万级融资44起，百万级融资2起，市场热度持续高涨。
- 从细分领域来看，网络安全、数据安全、云安全、业务安全、移动安全、工业互联网安全等领域投融资金额最多，成为网络安全投融资重点领域。

现状四：安全产业人才缺口巨大

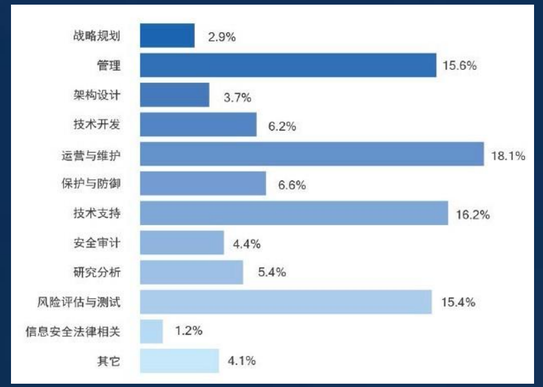
◆ 数量缺口巨大

- ✓ 我国设置网络安全类相关本科专业的高校116所，累积培养网络安全专业人才10万人
- ✓ 我国网络安全人才需求量为70万人，到2022年人才需求过百万

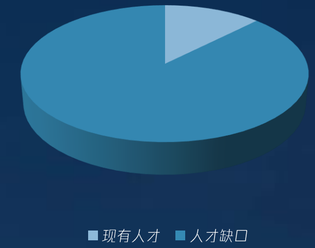
◆ 培养结构不合理

- ✓ 攻防两端人才分配不合理
- ✓ 运营与维护、技术支持、管理、风险评估与测试的人员相对较多，战略规划、架构设计、网络安全法律相关从业人员相对较少

网络安全从业人员工作岗位分布图

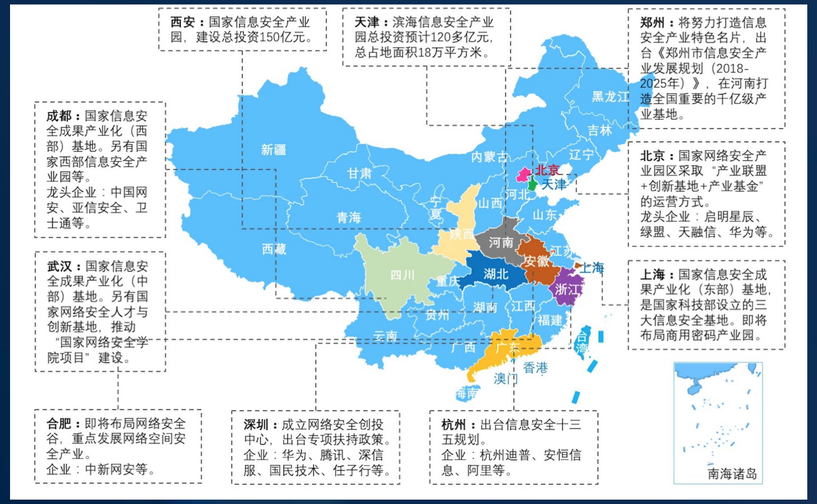


中国网络安全从业人员供需关系



数据来源：《2017年度中国信息安全从业人员现状调研报告》

现状五：安全产业园成为安全产业发展的重要载体



- 国内各地区加快布局网络安全基地，目前，北京、上海、成都、西安、合肥、深圳等城市已经布局了网络安全产业园；
- 结合现有网络安全产业园布局情况分析，人才基础丰沛的地区具有竞争先发优势。

目录

趋势一：市场范围呈现横纵向扩展模式

新兴领域

5G时代来临，物联网面临新的安全挑战

预计2021中国物联网市场规模将达到2.7万亿元，
其中物联网安全规模将达到301.4亿元，占比为1.1%。

企业上云步伐加速，云安全市场潜力巨大

预计2021年中国云计算市场规模将达到2066.3亿元
其中云安全规模将达到115.7亿元，占比为5.6%。

工业互联网安全防护能力薄弱，市场亟待挖掘

预计2021中国工业互联网市场规模将达到7988.3 亿元
其中工业互联网安全规模将达到228.0亿元，占比为2.9%。

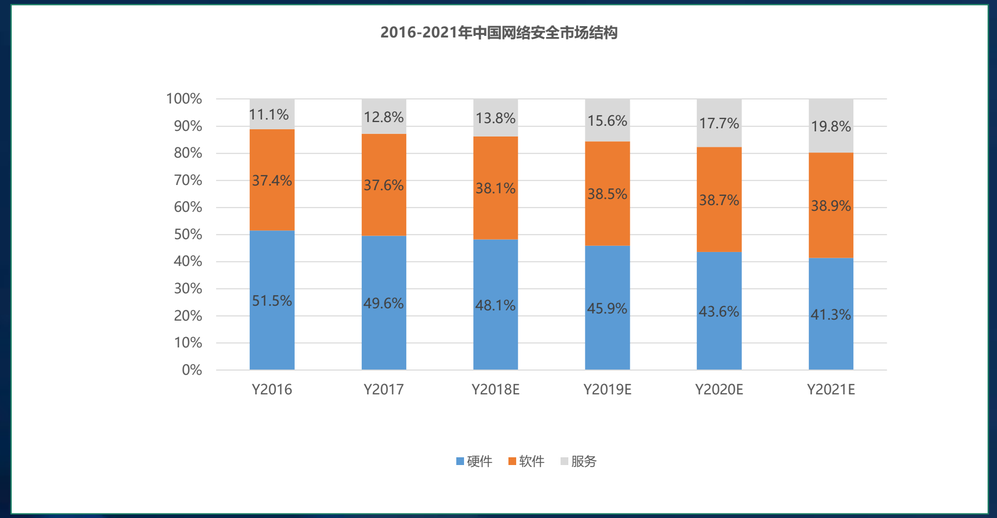
海外市场

- 欧美、日本等发达国家
  - 产品成熟度高、市场竞争力强
  - 具有创新潜力和海外市场销量
  - 标准化安全产品
- “一带一路”国家
  - 巴基斯坦等一带一路沿线欠发达国家网络安全需求量大且迫切
  - 加强沿线各国家区域安全合作，形成网安生态
  - 一体化安全平台及解决方案

SANGFOR 深信服科技 5911.1万元

NSFOCUS 7611.4万元

趋势二：市场由硬件驱动向服务驱动转化



趋势三：产业竞争从单打独斗到协同作战

单一功能产品 → 企业平台体系 → 产业生态联盟

网络安全企业构建完善的专业安全产品线，加强整体解决方案建设及安全服务。

启明星辰 Neusoft NSFOCUS 天融信 TOPSEC 蓝盾 BLUEDON Westone 卫士通

- 电子商务生态安全联盟
- 互联网金融安全联盟
- 威胁情报共享工程

趋势四：分析模式由传统模式向自动化模式转变

对海量安全数据进行攻击画像、威胁建模、情报匹配等自动化分析，形成完整威胁杀伤链可视化溯源，从而提升威胁发现与处置效率。

- 传统：安全问题出现—>客户反馈—>分析人员采集样本—>沙箱处理—>人工分析沙箱日志；
- 未来：自动从海量信息中寻找可疑数据，进行自动化智能分析评判，分析人员快速判断结果是否正常，最后新威胁迅速进入情报体系。

趋势五：防护思路从严防死守向应急响应转变

安全防护

业务连续能力

- 不间断可靠供给的能力

安全可控能力

- 保障网络信息安全的基本前提

数据安全能力

- 敏感数据及重要资产防护

结合

态势感知

数据汇聚、融合和共享

- 各层级数据汇集
- 基于关系挖掘深度融合
- 基于公平性的共享

态势感知分析

- 监管层和终端层相结合的态势感知
- 终端状态与网络实时通联行为结合

未知攻击发现

- 结合低位线索发现、中位关联定位、高位全局综合分析的大规模未知攻击全方位掌控

线索追踪

- 基于高中低位数据时空传导关联
- 结合现实人机画像实现人机结合追溯
- 拓展境内外协作体系和机制保障

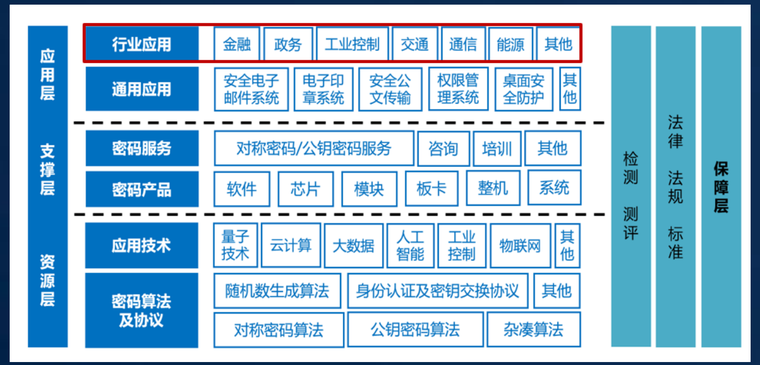
应急响应

- 评估风险、制定策略、拟定应急预案、演习并培训。

通过各种途径〔安全监测、信息共享、第三方通报等〕获知安全事件，对事件进行处理及恢复。

- 总结经验，调整安全策略，以防止安全事件再次发生。

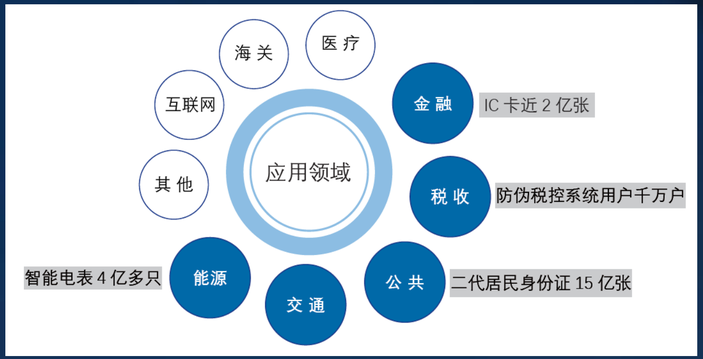
趋势六：金融和关键领域密码应用成为热点



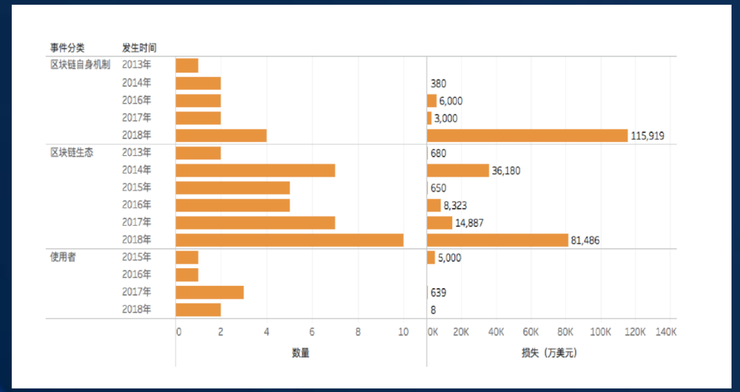
- 2017年4月13日，国家密码局就《中华人民共和国密码法（草案征求意见稿）》公开征求意见

  关键信息基础设施应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护，同步规划、同步建设、同步运行密码保障系统。

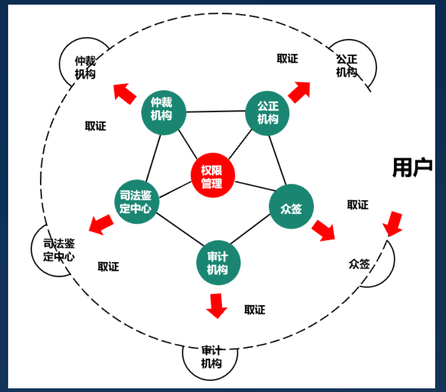
- 中共中央办公厅、国务院办公厅印发《金融和重要领域密码因公与创新发展工作规划（2018-2022年）》
  - ✓ 金融领域
  - ✓ 基础设施网络
  - ✓ 数字经济
  - ✓ 信息惠民密码应用



趋势七：区块链——提供安全新需求与技术新思路

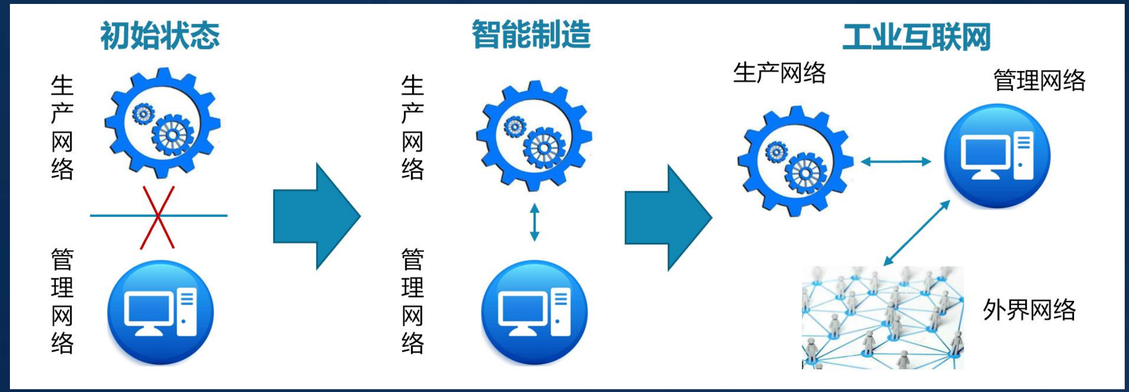


- 针对目前区块链存在的底层代码、密码算法、共识机制、智能合约、数字钱包等安全问题，该领域涌现出区块链安全新业态
- 区块链技术发展提供数字存证、版权安全保护新思路



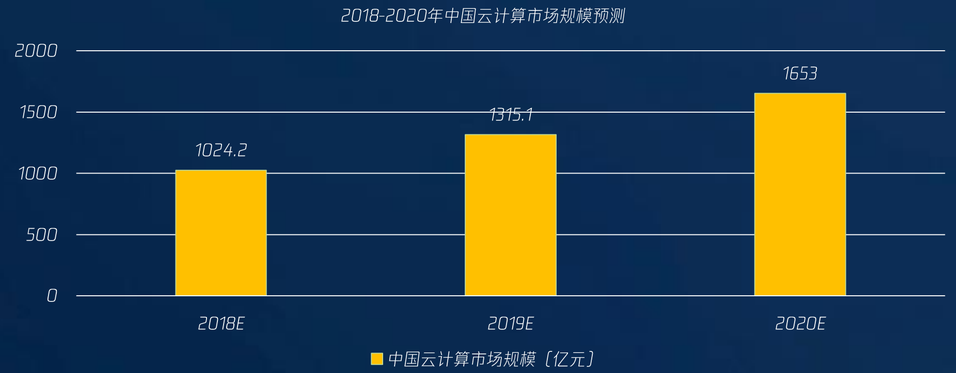
趋势八：工业互联网——安全从“IT”防护到“IT+OT”防护

- 工业企业安全意识薄弱，大多只在企业管理网络有所防护，但在工控领域的安全防护措施几乎为零；
- 2017年，工业领域信息安全市场规模为35.7亿元，仅占工业互联网市场的0.8%；
- 随着智能制造、工业互联网的快速发展，使得安全防护问题也加速暴露，安全防护范围向工控端扩展。

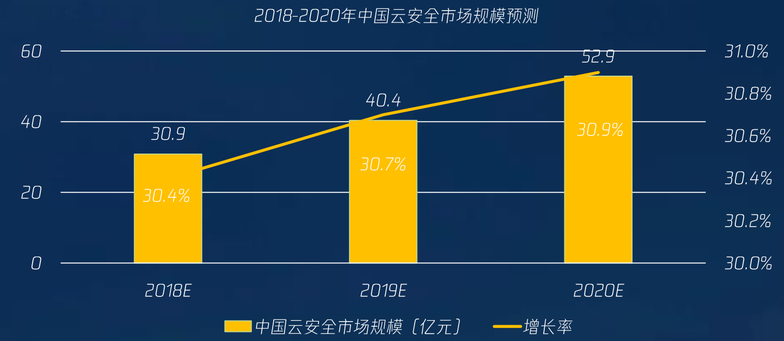


- 生产与管理网络完全隔离，没有任何安全防护手段
- 工业数字化使得生产与管理网络界限被打破，企业开始关注工控安全问题
- 工业企业加大与外界网络的互联互通，安全问题全面暴露，安全防护范围逐步扩大

趋势九：云计算——产业规模增长带动云安全市场突破

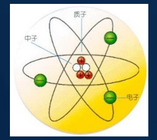


- 《推动企业上云实施指南》
- 《云计算发展三年行动计划（2017-2019年）》
- 等保2.0：《网络安全等级保护条例（征求意见稿）》



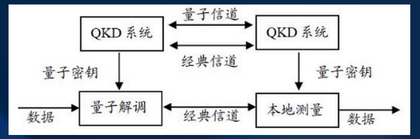
- 公有云领域，云服务厂商构建完备云安全能力体系。
- 私有云、混合云领域，网络安全厂商推出全方位安全解决方案。

趋势十：量子保密通信——从基础研究向产业化迈进



量子特性：
- 测不准原理
- 量子不可克隆原理
- 单个光子不可再分

量子保密通信主要是指利用量子状态作为信息加密和解密的密钥，在通信中并不传输密文，只是利用量子信道传输密钥，将密钥分配到通信双方。



上游

- 量子保密通信核心器件制造商〔光子源、光子探测器等〕
- 量子保密通信设备制造商〔网关、交换机等〕

中游

- 量子保密通信传输网络建设〔光纤搭建、基础设施、网络设施等〕
- 量子网络运营与应用〔量子通信网络运营、服务提供商等〕

下游

- 量子保密通信行业应用〔金融、军事、政务、商务等〕

国盾量子 QuantumCTek　DCITS 神州信息　中国有线　四创电子 SUN CREATE　KEHUA 科华恒盛
问天量子　中国通信建设　神州数码 Digital China　蓝盾 BLUEDON　NSU 新海宜 NEW SEAUNION

目录

赛迪建议：构建“产学研用测”五位一体生态体系

建立人才培养新模式
打造高校专业学科教育、职业技能培训、安全知识普及结合的人才培养体系

创新产业研发模式
在前沿技术研发、科研服务和创新孵化与科研成果转化三个环节发力
构建完善的产业研发体系

提升产品与服务能力
大力发展核心基础硬件
拓展信息安全产品范围
搭建安全服务创新平台

推进重点领域安全应用
金融、物联网、智能网联汽车、政务、大数据、人工智能、工业互联网

重视安全产品评测
创新检测服务模式
加强检测工具研发与推广
增加企业检测知识培训

腾讯全球数字生态大会
TENCENT GLOBAL DIGITAL ECOSYSTEM SUMMIT

Tencent 腾讯 | 腾讯安全 Tencent Security

感谢聆听