2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

未来核心技术与网络空间安全

沈寓实

博士，MBA，国家千人计划专家

清华海峡研究院智能网络实验室 主任

飞诺门阵科技有限公司 董事长/首席科学家

世纪互联集团（VNET）高级顾问/首席专家

中国云体系产业创新联盟 秘书长

未来信息技术发展趋势

未来信息世界发展的三大阶段

初级阶段——“物理集中”

效果是规模经济引起的“便利和效率”。

中级阶段——“化学反应”

效果是基于大数据的智能分析以协助决策和解决大规模商务、政务和社会问题。

高级阶段——“基因突变”

效果是将产生大量的基于高品质视频和多媒体智能的全新市场应用和服务，物理世界和虚拟世界的深度融合

信息产业螺旋发展趋势

“集中”

70年代开始的大型机时代

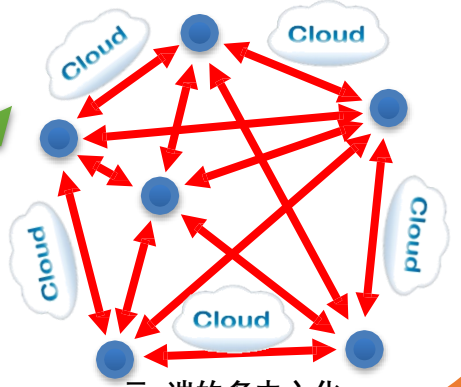
“分散”

90年代之后进入PC机

新的“集中”

国际已经形成7朵
大型公有云

新的“分散”



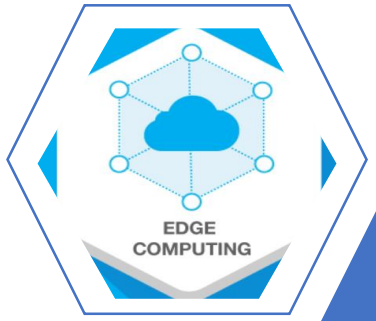
云+端的多中心化
边缘透明计算

未来即将到来

未来是精彩的边缘计算，我们要赶上第二次潮流的到来！

信息产业螺旋发展趋势：即将进入网络空间新时代！

新一代网络空间热点技术：ABCDE



云计算

人工
智能

边缘计算

大数据

区块链

数据中心发展趋势

下一代云应用及安全

软件定义基础架构

海底电缆着陆

私有云互联

下一代移动和物联网

数据中心发展趋势

- 全球数据中心平台与生态系统逐渐匹配
- 互连平台为实现面向互连的体系结构提供关键的构建模块
- 重新定义数据中心角色的关键技术日趋成熟

云计算发展趋势

私有云 Cloud → 混合架构 → 混合云 Cloud ← 提供了新的机遇 ← 公有云 Cloud

全球化基础设施的扩张加速

大型企业拥抱云计算

无服务器架构的普及

物联网（IoT） 有望爆发

- 云不再是一种独立发展的技术，而是成为各种创新应用全面融合的枢纽
- 云不再是一种尽力而为的互联网服务，而是成为智能社会最重要的公共基础实施

云计算发展趋势

软件定义是云计算的的关键技术

- Gartner总结2014年具有战略意义的十大技术，首次放入了**软件定义一切**。
- IDC预测，2014年至2018年，企业和云数据中心领域SDN的年复合增长率将达到**89.4%**。

传统的基础设施正在变革，并将迎来一个软件定义的黄金时代。这个时代将具备三个特点：从硬件向软件演进、软件服务崛起、以及开发者数量将持续增长。

——Martin Casado 2016.5 Interop大会

软件定义数据中心

软件定义存储

软件定义网络

软件定义架构

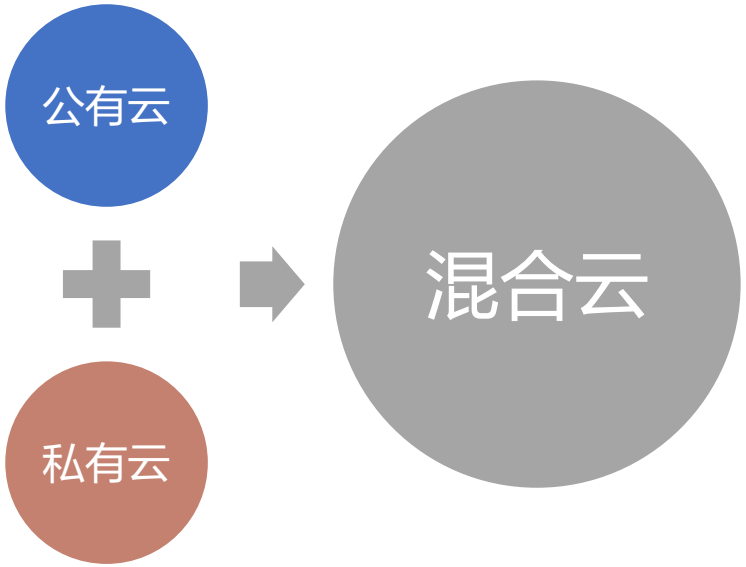
软件即服务

软件定义带来的好处：

- 提高网络资源利用率
- 实现网络虚拟化
- 促进云计算业务发展
- 提升端到端业务体验
- 降低网元设备的复杂度

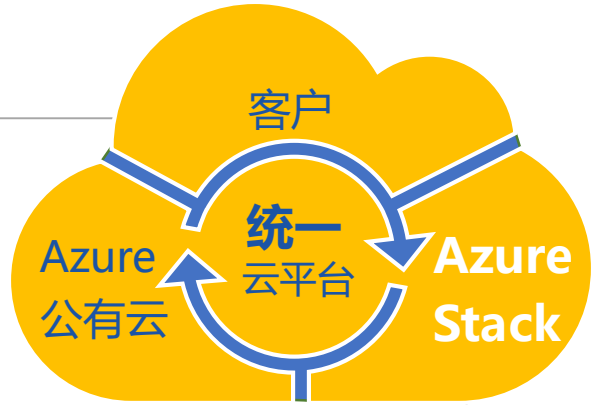
混合云是云计算发展的重要趋势

- 根据Gartner公司调查，2016年是许多大型企业开始投入混合云的关键年，至2017年底，**近半数以上**的大型企业都会有混合云环境。
- VMware、IBM、AWS、Azure等都已推出混合云方案。微软提出“**三云合一**”Cloud OS的概念，集成相关服务，为企业客户提供定制化云服务和行业大数据方案。



微软“三云合一” Cloud OS：

- Microsoft Azure
- Windows Server
- Microsoft System Center



微软“一云俱全”，提供从IaaS、PaaS以及SaaS的，85%的全球财富500客户正在使用的，支持Linux、MySQL、Hadoop等开源技术的可信云服务。

大数据发展趋势

数据总量呈指数型爆炸性增长

数据的结构发生了巨大的变化

数据的组织发生了巨大的变化

“大数据”是基于多源异构、跨域关联的海量数据分析所产生的决策流程、商业模式、科学范式和生活方式上的颠覆性变化的总和。大数据时代是数据外部化与人工智能的时代。

人工智能技术现状

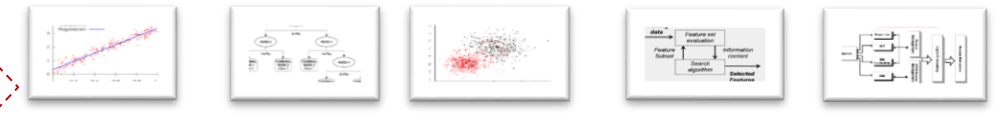
算法 —— 是人工智能兴起的决定因素，开源平台成为巨头抢夺生态的关键手段。

算力——通用计算机计算能力的演变，专用计算芯片是人工智能算法高效实现的保障，可重构计算与ASIC、FPGA的区别

机器学习算法梳理

三大通用任务：回归 | 分类 | 聚类

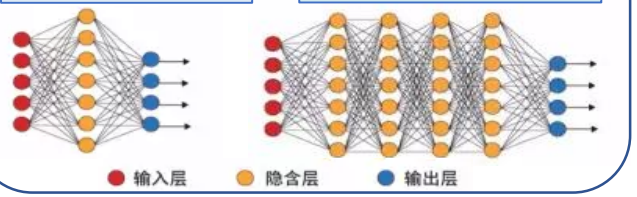
两大降维问题：特征选取 | 特征提取



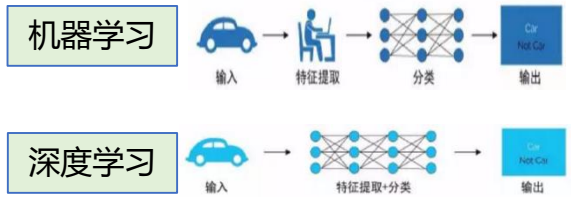
深度学习体系梳理：模型 | 优化算法 | 关键技术 | 网络结构

浅层神经网络与深度学习神经网络的区别

浅层神经网络 | 深度学习神经网络



机器学习与深度学习的区别



人工智能、机器学习、深度学习三者之间的关系

人工智能芯片的技术要素

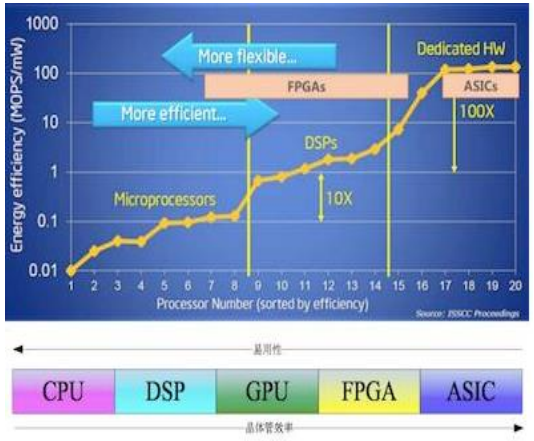
一． 可编程性：适应算法的演进和应用的多样性；

二． 架构的动态可变性：适应不同的算法，实现高效计算；

三． 高效的架构变换能力：< 10 Clock cycle， 降低开销；

四． 高计算效率：避免使用指令这类低效率的架构。

五． 高能量效率：~5TOps/W



人工智能的未来

弱人工智能

单一用途，只能模拟思维

- 多项选择、模式识别（图像识别、优化、搜索）
- 非常有用，在特定任务中要强于人类

强人工智能

通用人工智能(AGI)，拥有思维能力

- 进展很小，需要完全人工智能（AI-Complete)
- 如果没有（语义）理解能力是行不通的
- 约翰.麦卡锡（John McCarthy）预言5-500年

智能的未来（智人）

算法不太可能只被超人类掌控

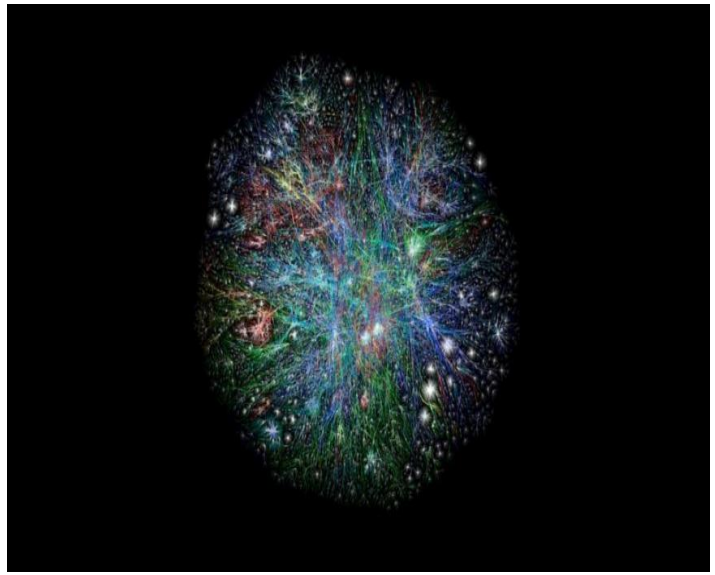
- Open AI, Partnership on AI, AI for Good…
- 需要管理的是数据
- 生命体可以被算法+数据重新定义吗？
- 我们能否提出一个新算法去解决所有的问题呢？

大数据 = 生产资料
云计算 = 生产工具
人工智能 = 生产力

- 人类和机器智能共同进化：计算机在进步并与大数据结合，是对人类智能的重要再创造
- 人工智能要达到科幻小说描述的情景还有很长的路要走，我们对人类智能的了解还不足够
- 未来之路：“人工智能+人类智能”(AI + HI)长期共存、协同发展
- 人类在相当长时间内将主导这一进程

区块链发展趋势

从信息传递到价值传递和共享，对下一代互联网定义



信任
依赖于算法

传递
避免重复支付

今天在不可信的网络上已经近乎完美地解决了信息传递。
但难以解决信任、契约与合同

还不能在不可信的网络上支持实现价值的点到点、机构与机构传递。
仍然依赖于中心机构记账

未来，由大家共同形成的网络来实现记账，而不是靠中央机构、牌照和批文，基于全网加密解决方案，在互联网上签合约

区块链解决了“少数服从多数”统一的数字表达

区块链创新与挑战

创新

去中心化、开放性、去信任、日常生活维护、信息不可篡改性、匿名性等特征，帮助企业降低行业信息不对称及交易成本、改善业务。这些特性似的其具有无限的潜力。

分布式账本

跨商业网络共享的只能添加的分布式记录系统

智能合约

交易条款内嵌在交易数据库与条款执行中，一定条件满足，可自动执行处理条款

信息追踪

保证适当的可见性；交易安全、真实和可验证即可

共识机制

所有参与的各方都同意网络中已验证的交易

资产安全风险

区块链资产存在系统漏洞那个、黑客攻击等安全风险

投机风险

区块链资产价格波动起伏较大，投资者投机风险较大

匿名风险

虽然区块链资产具有匿名性的特征，但仍在一定程度上存在匿名风险

反洗钱

存在部分人士利用区块链的匿名性进行洗钱

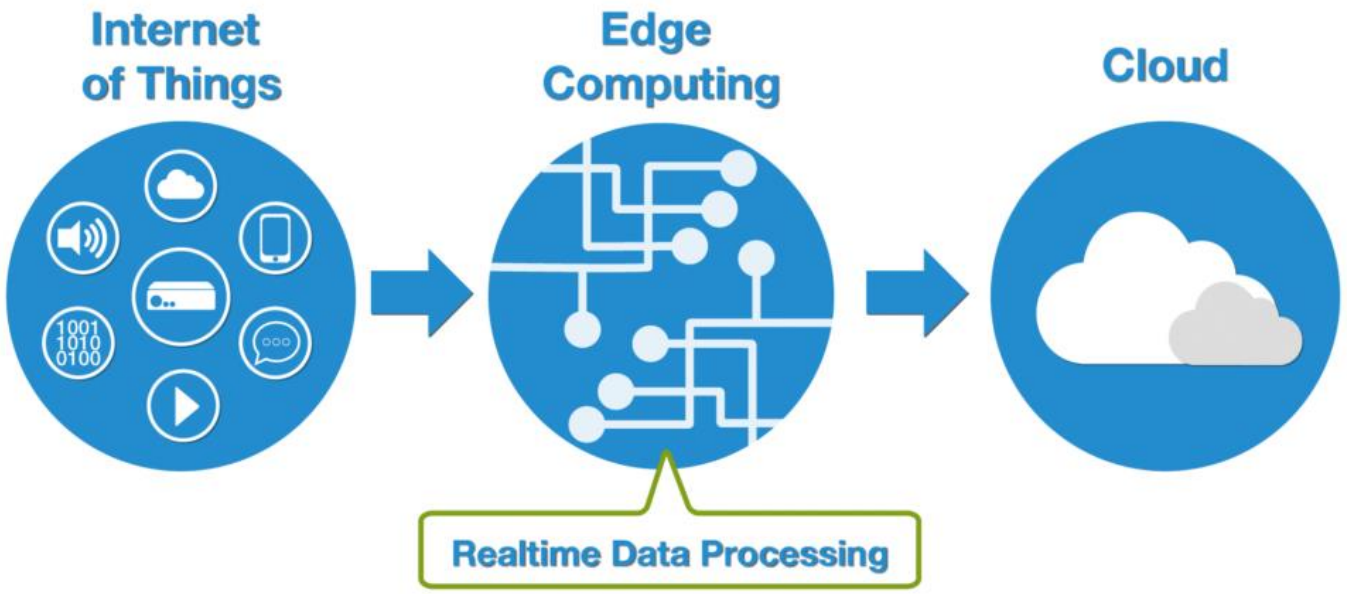
挑战

随着区块链被广泛应用，区块链资产交易呈现爆发式增长，但在发展的过程中，各方面仍存在一定的挑战。

边缘计算发展趋势

用网络边缘对数据进行分类，将部分数据放在边缘处理、减少延迟，从而实现实时且更高效的数据处理，达到对云计算的有力补充。

数据处理由网络中心下放到网络边缘的节点上。



- 数据处理更接近数据来源，可以减少迟延时间。
- 企业在本地设备的数据管理解决方案花费远比云上和数据中心少。
- 物联网设备的增加，使得网络带宽更加有限，造成数据瓶颈。

IoT + EC

一个工业级单元应用物联网的传感设备将平均超过10万个，如此大量的数据如何解决**存储、耦合、移植、分析**，而且必须实时性要求达到毫秒级。
边缘计算对于**数据整合、数据预处理、数据集成**起着至关重要的作用。

5G + EC

2020年5G商用，理论峰值可达到每秒数GB，如果**一个5G局域网**没有**一个专属的云存储数据节点**，再快的数据传输也是噱头。
速度虽然飞快，但若对5G下的传输数据进行分析也是一种灾难，所以在数据传输前需要预处理，将**数据抽象化、碎片化、结构化**，这就体现了边缘计算的重要性。

2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

新一代网络计算体系助力“新基建”

新基建的三个维度

数字工程：新基建本身的价值创造

由5G、大数据、人工智能、云计算、物联网、区块链、工业互联网等数字化基础设施本事投资和发展组成。这是新时代的“电力”和“石油”。发展模式以轻资产、高科技含量、高附加值为主。

融合工程：新基建的融合颠覆功能

经过数字化、智能化改造的传统基建（如智慧城市、智慧交通等），对各行各业进行颠覆；弥补某些传统基建“短板”的新型细分领域，如：交通运输领域（轨道交通、冷链物流），能源行业（核电、特高压）等。

创新工程：新基建的融合创新功能

由数字基建引发的新兴产业及全新配套设施，包括新能源、新材料及其应用领域（光伏、生物质能等），无人机配套设施（无人配送物流、无人化防疫等），高新技术产业园（新的生物医药工程、卫星太空基建等）。

五全信息——新基建颠覆行业的基因

五全信息

- 全空域泛在的信息
- 全流程持续的信息
- 全场景活动的信息
- 全智能解析的信息
- 全价值叠加的信息

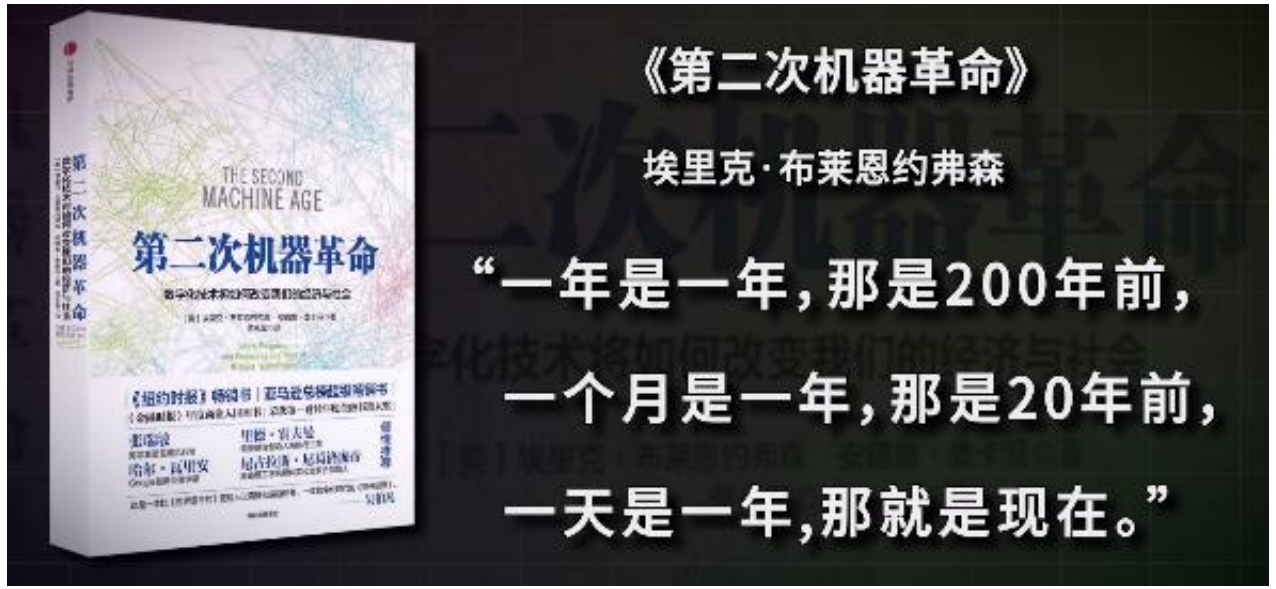
全维度数据采集

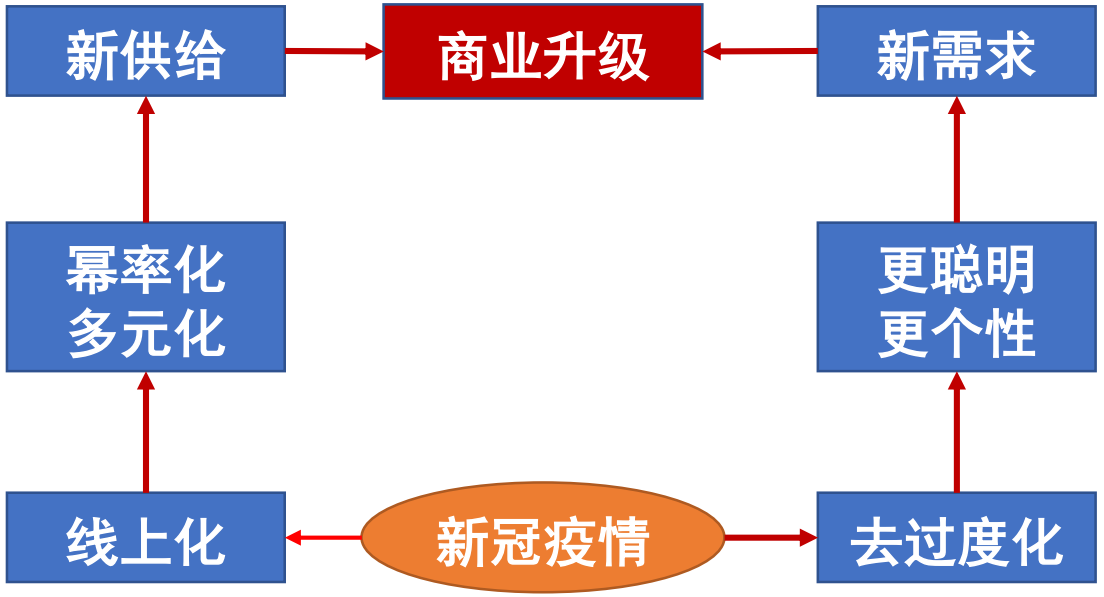
多维度数据挖掘

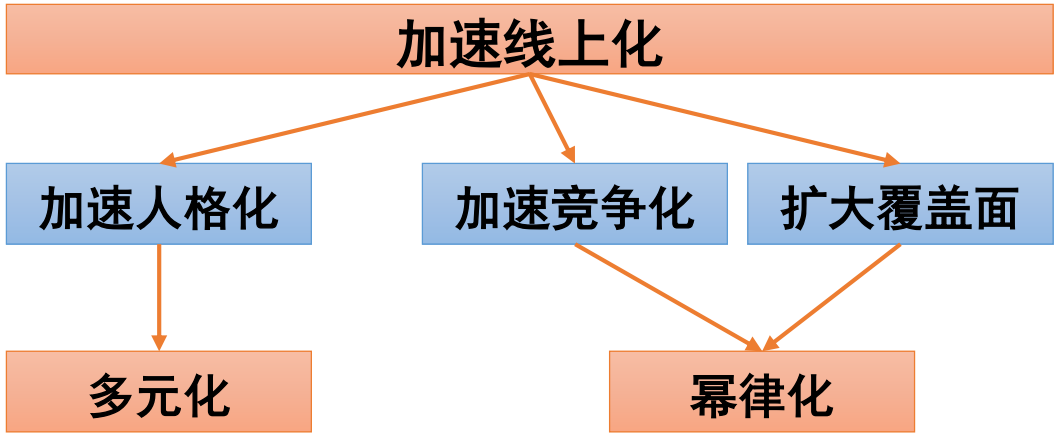
价值叠加颠覆行业

这五种信息一旦产生，在各行各业就会产生资源优化配置，产生效益，产生新的生产力，即我们所说的颠覆性功能。

2020年中国科技发展的新趋势







“深挖洞、广积粮”
“大三线建设”
“两弹一星”

原材料资源保障
内需内供经济循环保障
核心技术自主创新保障

中国在高附加值行业，比如半导体、医疗器械、5G通讯等领域产生大量新机会！

“新基建”带来产业新机遇

“新基建”：主要指**以5G、人工智能、工业互联网、物联网**为代表的新型基础设施，本质上是信息数字化的基础设施……能支撑传统产业向**网络化、数字化、智能化**方向发展的信息基础设施，包括新一轮的网络建设，如光纤宽带、窄带物联网等；数据信息相关服务，如**大数据中心、云计算中心以及信息和网络的安全保障**等，也必将成为我国 “新基建” 的核心所在。

以**非冯诺依曼网络计算体系**的研究为基础，面向5G、边缘云计算和人工智能等领域，联合行业头部企业及产学研资源，构建智能化边缘云计算平台，降低软硬件成本和建设周期，**积极参与智慧城市、5G应用、区块链、物联网应用等落地项目**，使异构人工智能网络平台技术真正地在实际应用中发挥自身优势。

人工智能时代的网络计算通用构架

工业时代

电力决定城市的工业发展上限。

全新计算架构研究的黄金时代！

中国引领第四次工业革命的机遇！

摩尔定律将失效

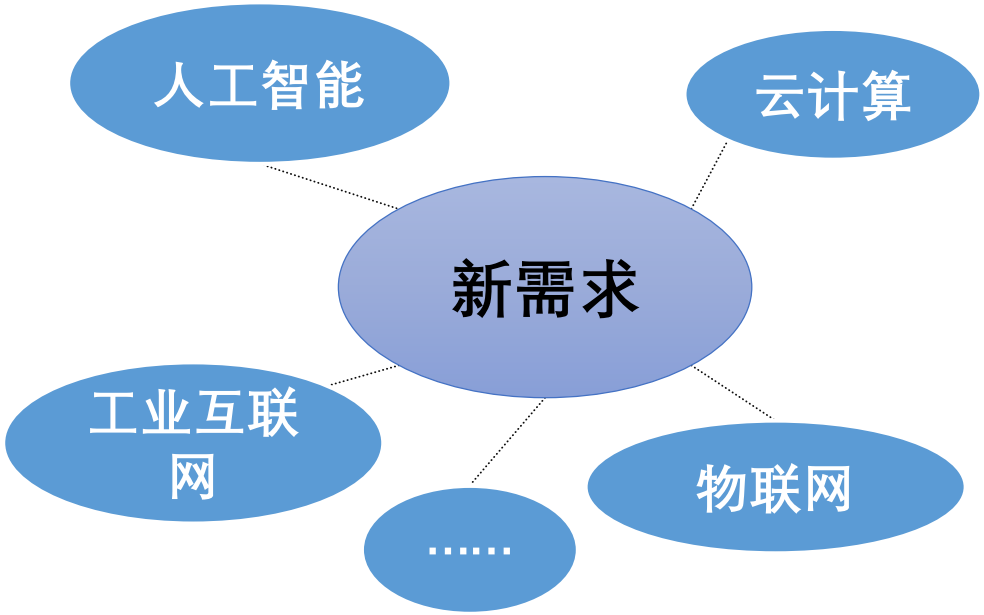
冯·诺依曼瓶颈

超强算力成为智能计算飞跃的拐点，智能网络计算系统的性能提升，未来30年有望达到100万倍。

摩尔定律 ↓ 并行计算

智能时代

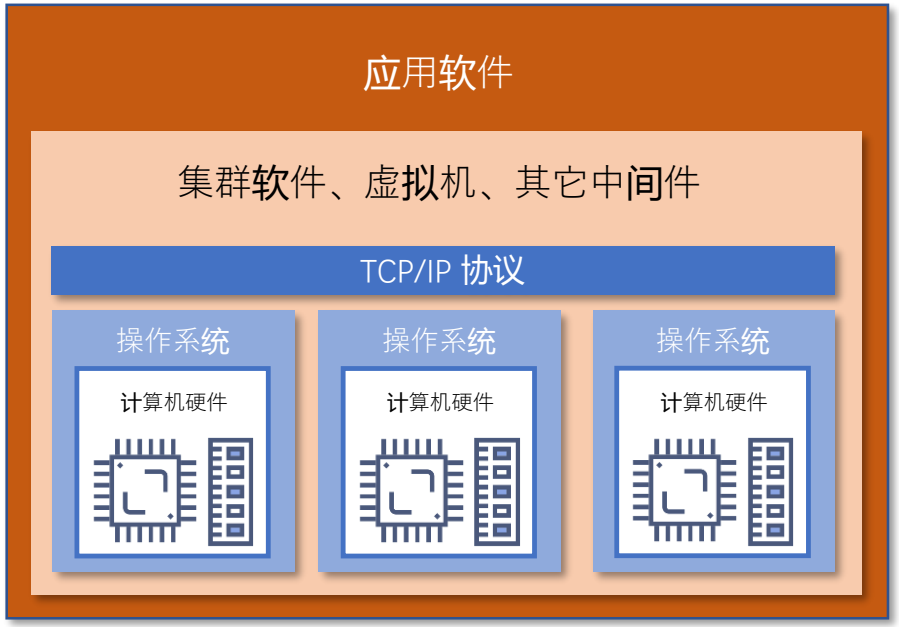
算力决定城市智能化水平上限。



设计面向**未来的网络计算架构**，从根本上提供一个高质量的网络服务环境，进一步形成**自主可控的未来网络产业生态链**，将极大地支撑我国在未来网络领域**跻身创新型国家前列**。

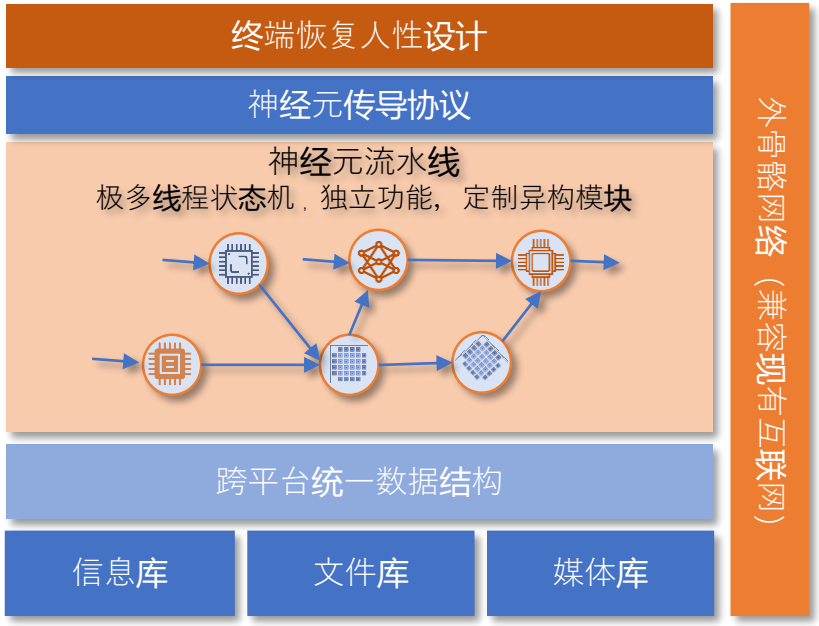
非冯诺依曼计算—突破计算、通信、存储的瓶颈

基于冯诺依曼结构和TCP/IP协议的网络计算体系



VS.

基于非诺结构网络计算体系



CPU	IP协议	软件危机
并行深度受限；**病毒的根源**：用户文件可搭载电脑程序，用户数据和电脑程序同时存放在CPU的储存区	尽力而为；**高延时**；**黑客的根源**：未经许可就能向任何地址发送任意数据包	并行编程带来的**手艺困难**；高效的操纵多核平台以取得更好的机能，必须对计算机的硬件有较深切的理解

流水线结构	传导协议	统一数据结构
独立的**时间扩展、空间扩展、功能扩展、资源扩展**；执行任一维度的扩展不影响其他维度；且**不增加软件复杂度**	**地址+功能+权限**；可管理的开放；网络业务流程完全开放；监管措施与用户设备完全隔离，**绝对安全**	解构传统数据库；**软件硬化**；无数设备互联；**异构设计**；剥离多媒体文件

核心技术“弯道超车”的历史机遇

习近平强调：实践反复告诉我们，关键核心技术是要不来、买不来、讨不来的。只有把**关键核心技术掌握在自己手中**，才能从根本上保障国家经济安全、国防安全和其他安全。

人工智能、大数据、云计算催生第四次科技革命， 将重度**解放人脑**，而被释放的脑力资源终将被再次投入创造和娱乐两个方向，同时对支撑计算、存储、通信**算力升级**提出进一步需求。

中央定调「新基建」， **5年35万亿元**投资发力于科技端的基础设施建设，主要包含 5G 基建、特高压、城际高速铁路和城际轨道交通、新能源汽车充电桩、大数据中心、人工智能、工业互联网等七大领域，涉及到通信、电力、交通、数字等多个社会民生重点行业。

是因为**云计算**时代使**Linux**类开源云操作系统的地位日益提升，终将**弱化**Windows、安卓等个人操作系统的**垄断**。

我国在**通信芯片**领域近年一直呈**赶超之势**。南京网络通信与安全紫金山实验室已研制出CMOS**毫米波**全集成4通道相控阵芯片，成本降低50倍，**国际领先**。

随着开源芯片生态的建立，我国在**专用芯片**领域与西方的**差距**已日益**缩小**， 受制于西方已久的局面不仅有了重大转机，有足够的西方先进经验可以学习，也是我们的**后发优势**。

核心技术突破是网络空间安全保障

没有网络安全就没有国家安全

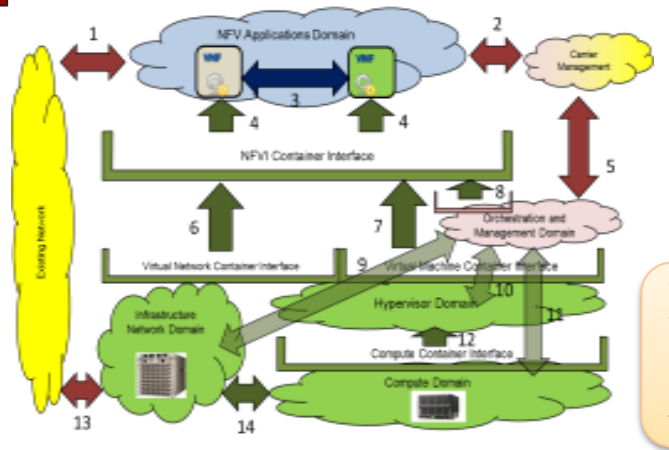
- 保护政府信息主权，企业数字产权，个人隐私权，提高安全保障能力，自主掌控业务数据，以及对应新技术带来的安全挑战是客户（包括政府，运营商，企业，消费者用户）最关注的问题。

➢外国间谍网络监听

客户面临的担忧和挑战

➢网络犯罪分子攻击

➢内部人员商业泄密



➢新技术安全挑战（NFV、SDN、5G 、云计算、大数据等）

网络安全的六大维度

- 各维度中都需要国际合作，跨界合作，跨部门合作

➢国际政治

“没有网络安全，
就没有国家安全”
…

➢国家法律

网络实名制，
个人数据保护法
…

➢行业标准

CC，ISO，CSA，
3GPP/GSMA…

➢管理流程

安全战略，
组织架构，
业务流程，
管控机制

➢技术工具

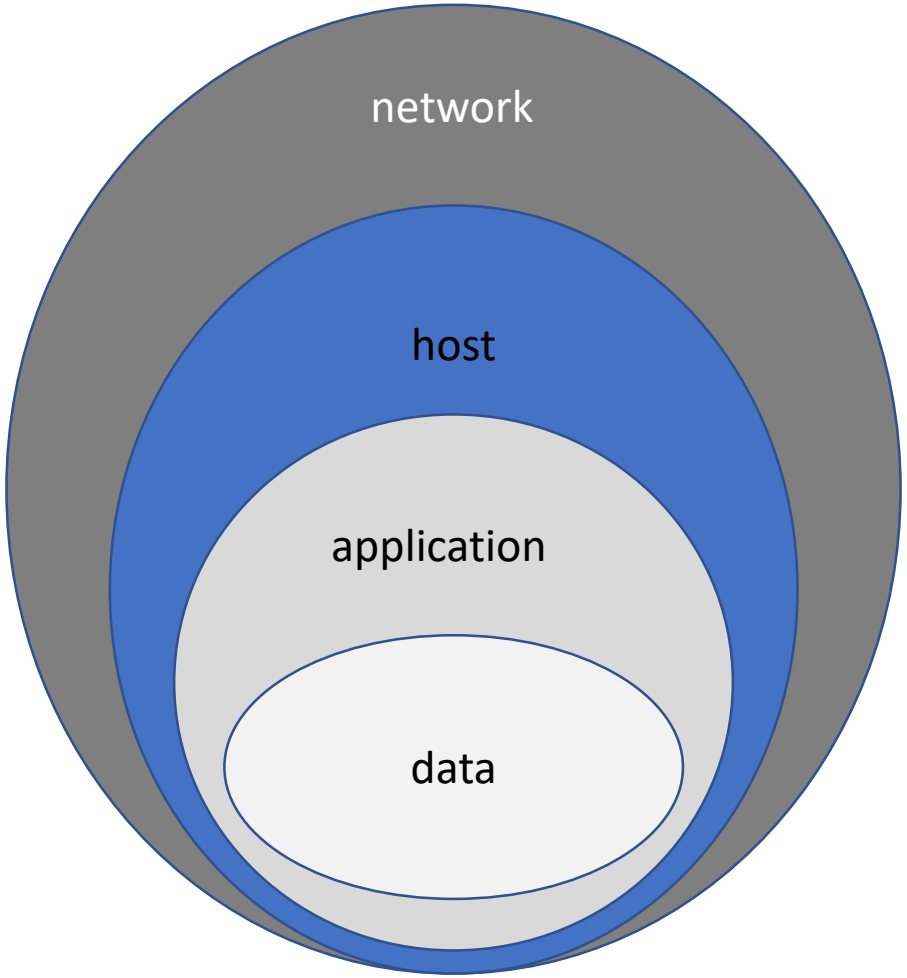
安全架构，
安全方案，
安全协议，
测评工具

➢人才培育

技能培训，
资格认证，
工作经验，
大学教育

新一代安全理念

- 数据是新中心：一切安全活动都应该是围绕业务数据
- 身份权限是新边界：防火墙已经不是安全边界
- 行为是新控制：补丁、基线、策略已经不能控制人的行为，深度学习才是安全控制的趋势
- 大数据情报分析是新服务：安全日志就是安全情报，基于大数据的安全分析，安全态势感知及可视化才可落地，信息安全已经互联网化
- 安全是体系的构建：要基于纵深进行整体防护而非单点堆叠防御



防护纵深的“洋葱”模型

加速网络空间国际合作

生存新空间、精神新家园、治理新领域、经济新沃土、文化新载体、外交新途径、作战新阵地。

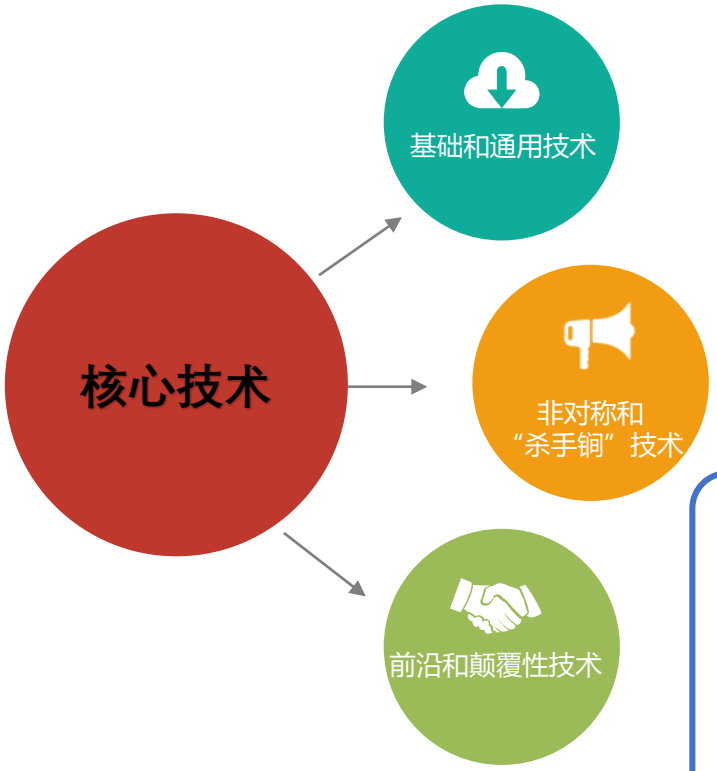
网络强国格局道义力量之国际合作：构建网络空间命运共同体；网络空间“和平共处原则”。

“数字立国”的基础

- “数字立国”的“两大途径”：国家网络空间治理体系和治理能力现代化、网络空间法制化。
- “数字立国”的“五大力量”：号召力、执行力、生产力、文化力、国防力。
- “数字立国”的“三大抓手”：网络强国战略、大数据战略、“互联网+”行动计划。
- “数字立国”的“中国目标”：网络安全和信息化为一体之两翼、驱动之双轮的网络强国。
- “数字立国”的“世界目标”：构建网络空间命运共同体

1. 处理“两大关系”：国家与人民的关系、军队与地方的关系
2. 服务“三大目标”：网络强国战略、大数据战略、“互联网+”行动计划
3. 把握“四大要素”：逻辑、物理、行为、信息
4. 防范“五类风险”：政治风险、军事风险、经济风险、文化风险、外交风险
5. 坚持“六大原则”：回归原则、补缺原则、优化原则、前瞻原则、关联原则、技术原则。
6. 聚焦“七个重点”：主权、发展、安全、文化、国防、法制、合作

什么是核心技术



一是基础技术、通用技术。
二是非对称技术、“杀手锏”技术。
三是前沿技术、颠覆性技术。

典型之一：
芯片和操作系统：是构建信息技术产品和系统的基础，也是我国突破核心技术受制于人的焦点。

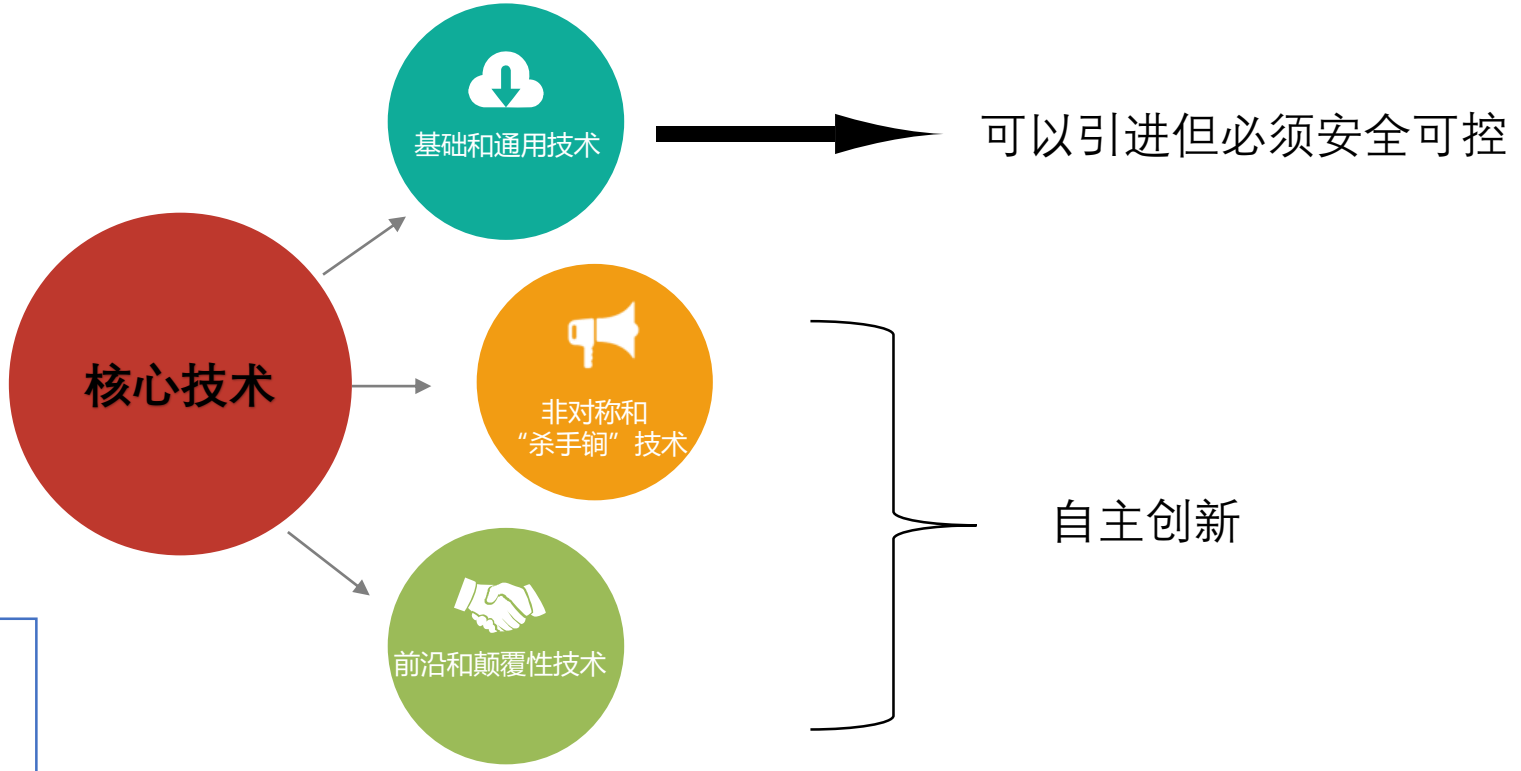
典型之二：
网络攻防类技术：网络空间具备明显的攻强守弱特性，在难以有效防御美国网络监控、网络攻击等手段的情况下，我们要形成网络攻击追踪溯源等有较强威慑力的技术手段和能力。

典型之三：
量子计算、生物计算等颠覆现有计算体系的技术，这是能够使得我们在新一轮信息技术发展竞技场中取得先机、掌握游戏规则的关键。

如何突破核心技术？

我们不拒绝任何新技术，新技术是人类文明发展的成果，只要有利于提高我国社会生产力水平、有利于改善人民生活，我们都不拒绝。问题是要搞清楚哪些是可以引进但必须安全可控的，哪些是可以引进消化吸收再创新的，哪些是可以同别人合作开发的，哪些是必须依靠自己的力量自主创新的。

——网络安全和信息化工作座谈会



但必须解决安全可控问题

- 没有网络安全就没有国家安全。
- 网络安全和信息化是相辅相成的。
- 安全可控的核心就是解决开放环境下核心技术受制于人问题。

网络空间安全核心技术研究

提升网络空间安全可信的两种途径

传统思路：“有病治病”

- 补漏洞：对出现的安全攻击，打补丁方式解决单一问题

新思路：“增强体质”

- 另辟蹊径：从网络空间体系结构解决互联网安全可信的问题

网络安全攻防技术

- 网络与系统自动攻防技术
- 网络基础设施与基础协议的脆弱性分析与利用技术
- 全球网络安全测量、态势评估与威胁情报分析系统

安全可信的体系结构

- 以IPv6地址驱动网络AND作为互联网安全可信的基础
- 基于区块链和安全网络的三元计算和可信网络
- 基于面向连接的视频网络的新构架

工业互联网成为发达国家重塑制造业竞争优势的关键

工业互联网是实现制造业智能化的核心，目前全球主要国家正**加快工业互联网战略布局**，以抢占未来制造业竞争的制高点。

美国：先进制造战略

- **先进制造战略**
- **工业互联网/CPS**：先进制造战略的重要创新方向和基础

美国是利用基础科学、工业、信息技术、互联网等领域的综合优势，构建全球性的生态体系组织，从大数据应用等“软服务”切入，带动工业全流程、全环节竞争力的整体提升。

德国：工业4.0战略

- **工业4.0战略**
- **工业互联网/CPS**：工业4.0的核心基础

德国重点是基于制造装备、工业自动化、工业软件等方面的领先地位，通过全工业体系的协同（研究机构、协会、大学等），强化“硬制造”优势，同时拓展“软服务”能力。

无论美德使用何种名词，均将**工业互联网**作为变革工业和确立竞争新优势的技术基础，注重将顶层设计与优势企业主导相结合，强调**网络为基础、数据为核心**的作用，加快相关领域标准化进程。

科技创新与社会进步

三大社会问题

- 日益加剧的收入与财富分配不均（包容性增长）
- 社会流动性下降与阶层固化
- 可持续发展

科技创新如何推动社会进步

- 以科技创新促进社会的和谐发展与进步
- 成为弘扬社会创新的一个重要平台和引领者

全球视野与全球担当

打造全球资源整合型企业

- 以全球视野以及打造全球资源整合能力来应对全球变革带来的挑战
- 产生一批真正可以竞合全球市场的企业，支持“一带一路”战略

解决全球性问题

- 不仅要为中国的经济发展与社会进步继续做出贡献，更要为全球发展的重大挑战贡献智慧与解决方案
- 产生具有全球影响力的科技发展与创新


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音