互联网安全领袖峰会
Cyber Security Summit

腾讯安全
Tencent Security

腾讯生态安全研究中心
Center for Eco-Security Research

中国产业互联网安全发展研究报告

P17安全领袖俱乐部
腾讯生态安全研究中心

前 言

习近平总书记在“4.19 讲话”中明确指出：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大群众利益也难以得到保障”。互联网深刻改变了人们的生产和生活方式。经过 20 几年的发展，我国已成为网络大国，但还不是网络强国，尤其在网络安全方面依然面临严峻挑战，网络安全已经成为事关国家安全的重大战略问题。

网络安全在国家战略地位提升的同时也为经济发展提供支撑。随着互联网对于各个行业领域的渗透，产业互联网特征愈加明显。产业互联网服务涉及第一、二、三所有产业。连接对象方面，包括个人、企业及第三方机构；服务模式方面，产业互联网覆盖从企业产品生产到个人消费的全流程支持；技术架构方面，会涉及人工智能、大数据、云计算、物联网等多项技术，支持服务的实现。可以说产业互联网的发展将网络安全地位提升至新的高度。

本次研究以国家网络安全形势为基础，产业互联网发展趋势为导向，针对我国网络安全现状、趋势、问题进行研究，并提出对策建议。研究调研走访了国内主要网络安全服务商，希望本次调研能够为政府网络安全政策制定、企业网络安全发展规划以及社会网络安全认知提升提供支持。

受编写者水平限制，本次报告内容难免有纰漏之处，如有问题，欢迎读者批评指正。

腾讯生态安全中心

2019 年 7 月

目 录

报告核心观点

（一）网络安全已成为国家战略的组成要素和安全保障

世界经济论坛发布的《2018 全球风险报告》指出，网络安全已经与环境退化、经济紧张和地缘政治一起被列为未来面临的四个主要风险。伴随着互联网对于各个行业领域的渗透，产业互联网服务涉及第一、二、三所有产业，更是将个人、企业及第三方机构等所有对象连接在一起。网络攻击造成的影响已经从虚拟世界扩大到现实世界，网络安全已成为国家战略的组成要素和安全保障。

（二）国家 22 部委出台法律法规近 200 部，加速产业互联网安全发展

在产业互联网发展过程中，我国网络安全相关法规、政策呈现出系统化、及时化、产业化三方面特点：一是网络安全保障体系逐步完善。截止 2018 年，我国政府制定网络安全相关法律共 24 个，制定法规 11 个、规范性文件 136 个，共有 22 个部委参与；二是政策出台紧随网络安全形势变化。通过法律法规、指导意见、管理条例、通知规定等各种方式保障网络安全管理的及时性；三是网络安全产业化特征逐步明显。在传统网络安全基础之上，持续加大对于产业安全的保障力度，如《网络预约出租汽车监管信息交互平台运行管理办法》、《快递暂行条例》、《关于加强对电子商务领域失信问题专项治理工作的通知》等。

（三）IT 基础设施安全保障难度提升，未来市场投入将提速

伴随我国信息化建设的不断推进，金融、能源、交通、电信等重要行业系统普遍面临着推进信息化发展和防范安全风险的挑战，主要受部分技术依赖进口信息产品、数据安全的高标准要求、云安全的挑战、可信身份的建设以及新兴技术快速发展的潜伏风险等因素影响，使得关键基础设施的保障难度加大，各行各业在未来将进一步加大安全投入，提升保障能力。

就目前情况而言，我国网络安全主体投入仍然偏低。据 IDC 预测，2019 年中国安全解决方案总体支出将达到 69.5 亿美元，2018-2022 年预测期内的

年复合增长率（CAGR）为 25.6%，增速远高于全球平均水平，到 2022 年，市场规模将增长至 137.7 亿美元。

（四）各行各业积极上云，云安全服务市场进入高速发展期

产业互联网推进过程中，我国信息化建设已然呈现出“万云”共台的形势，政务云、企业云、教育云、健康云等各“云”汇集。由于传统安全防护措施不能满足云环境提出的安全需求，云安全服务正在成为信息安全行业一个潜力巨大的新增市场。P17 预计，未来 3-5 年，云安全服务市场的增速将高于信息安全市场的整体增速。

对于企业来说，上云有助于降低安全成本，这使得他们愿意在云安全上进行投入。因为成熟的云服务平台在响应速度以及应对整体网络威胁形势复杂性上，比传统 IT 架构更具优势。对于传统 IT 安全企业而言，顺应互联网基础设施“云”化趋势，立足已有产品进行转型，将安全能力云化，通过订阅模式进行交付，也将获得新的增长空间。

（五）安全与业务深度融合，激发产业新场景安全需求

产业互联网的东风下，大数据、物联网、人工智能的发展，促进网络安全在不同场景的应用更为广泛，企业业务、设备、网络融合程度持续提升，不同安全主体和网络的融合加深。这意味着产业升级过程中，每产生一次技术创新都必须考虑安全因素，每产生一个新的需求都默认包含安全需求，安全建设与业务流程深度融合。过去企业是“从安全的角度看待业务”，现在则是“从业务发展的角度看待安全”，企业需要以数据资产为中心构建业务安全防护体系，尤其是要预防不断扩张的黑灰产引发的薅羊毛、金融欺诈、广告点击欺诈、拖库撞库等业务安全问题。

（六）产业互联网时代，安全建设成为 CEO 一把手工程

与传统互联网的防御性安全保障不同，产业互联网与业务运营的深度结合，标志着安全融入到企业供应链、生产、销售、服务等各个环节。这也意味着企业的安全建设不再只是 CIO（首席信息官）和 CISO（首席信息安全官）的事情，上升为企业 CEO 一把手工程。企业的 CEO 需要牵头以战略视角进行

安全规划，从情报、攻防、管理和规划维度，构建企业的“安全战略观”，将过去被动防御的模式升级为主动防御体系。

（七）前沿科技将被广泛应用于安全技术

伴随着人工智能、5G、大数据、云计算、量子通信、区块链等前沿科技在产业互联网时代日臻成熟，网络安全技术也迎来新的发展趋势。网络安全中颇为重要的态势感知技术，将在大数据和人工智能的加持下，进一步提升效率、精准率，并降低成本；包含卷积神经网络在内的机器学习模型应用，给病毒对抗带来全新的思路；云计算的普及，让纵深防御（DID）、软件定义信息安全（SDIS）、安全设备虚拟化（SDV）成为潮流等。

（八）产业互联网安全整体人才储备不足，高端人才稀缺

产业互联网时代新增的安全需求以及更精细的安全分工，需要更为丰富的安全人才资源支持。但目前，我国网络安全人才培养与行业需求严重脱钩。首先，整体网络安全人才供给不足，截止目前我国培养专业网络安全人才 10 万人，预计到 2020 年，网络安全人才需求将达 140 万人；其次，高端网络安全人才匮乏。产业互联网安全对于技术性和实践性要求较高，目前的人才培养模式无法完全满足网络安全需求。产业互联网安全人才，需要在安全技术以外，深入了解垂直纵深产业的业务、流程、设备。

（九）共建产业安全生态势在必行

共建安全生态的价值在产业互联网时代尤为凸显。产业互联网时代，各方都是安全生态构建的参与者，政府、网络安全企业、第三方机构分别在战略规划、技术研发、形势研判方面承担相应的责任，需合力保障产业互联网安全的健康发展。

聚焦在核心的网络安全攻防层面上，网络安全企业携手共建生态，不仅将共享彼此的威胁情报，提升攻防能力；还将有助于提升网络安全行业资源的配置效率，形成良性竞争环境，从而更好地为企业提供安全服务。

（十）产业互联网重塑安全服务供给模式：卖“产品”到卖“产品+服务”

产业互联网时代，网络安全建设不单纯是技术问题，还是管理问题。企业安全建设不仅需要有效的工具、科学的方法还需要专业的运维。愈发严格的政策及合规要求，和愈发复杂的威胁情况，使得企业迫切需要一套包含合适的人、工具、方法的安全服务模式，从前期就做好安全战略规划以及安全政策咨询。未来，企业对安全规划服务的需求将进一步增强。这意味传统的售卖软硬件安全产品的模式将不再适合，网络安全企业需要通过“专家服务”+“产品”的形式，帮助企业提升安全竞争力。

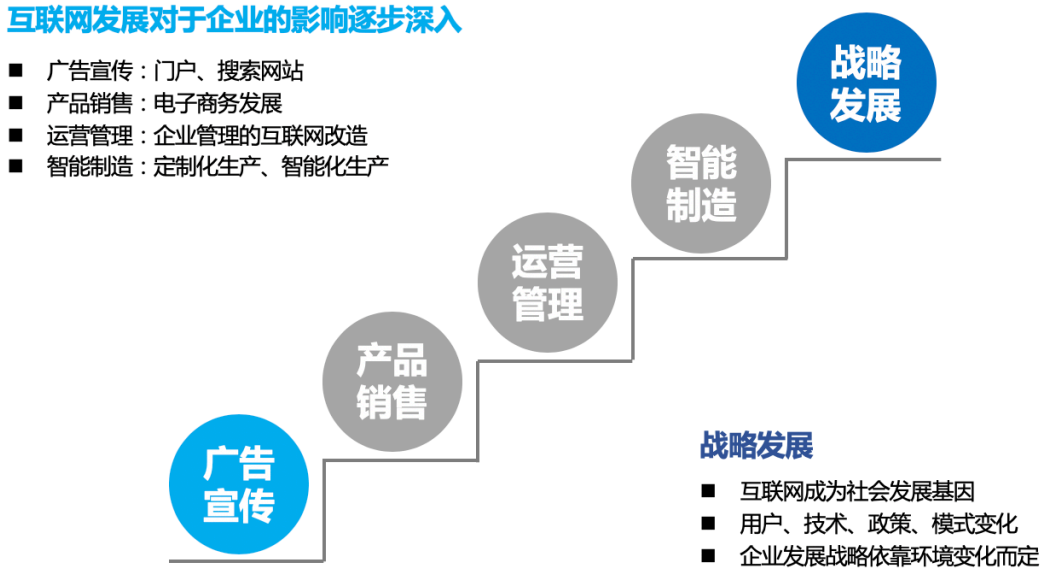
第一章 产业互联网发展与网络安全需求

一、产业互联网发展趋势

（一）数字经济成为我国在创新发展阶段的数字增长动力

根据迈克尔波特国家发展论，国家发展会经过三个阶段：第一阶段为要素推动的发展阶段，主要依靠劳动力、土地和其他初级要素成本优势推动经济增长；第二阶段为投资推动发展阶段，依靠大规模的投资促进经济发展；第三阶段为创新推动阶段，依靠提高资源生产效率的知识和方法推动经济增长。目前我国已经步入创新阶段，互联网为代表的信息技术已然成为创新和经济发展的主要力量，2018 年我国数字经济规模达到 31.3 万亿元，占 GDP 比重达 34.8%。在此背景下，信息技术及其产生的价值安全保障需求强烈提升。

（二）互联网基础应用环境完善推动其向战略实施融入



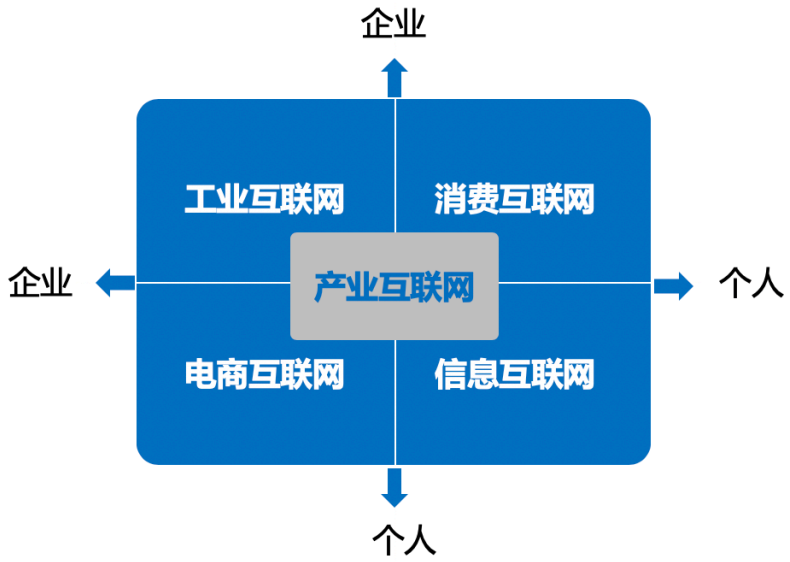
《中国产业互联网安全发展研究报告》

经过二十几年的发展，中国互联网对于政府、企业、网民服务趋于成熟。一是网民基础建立，截至 2018 年我国网民规模达 8.29 亿，普及率达 59.6%；二是应用范围广泛，我国市场上监测到的移动应用程序（APP）在架数量为 447 万款，服务涵盖衣食住行等各个方面；三是企业改造明显，自互联网发展初期，其先后完成了对于企业的广告宣传、产品销售、企业管理、生产制造等方面的改造，

目前互联网已经融入到企业战略制定层面。

（三）产业互联网是互联网发展功能和特征的融合体现

中国互联网从功能角度总结为四个方面：一是信息互联网，以互联网公司为服务主体，个人间信息传递为主的、提供以提高信息传递效率的信息产品和服务，如广告、新闻、搜索、社交等；二是销售互联网，以电子商务为代表的应用提升企业产品与消费者的连接和销售效率；三是工业互联网，利用互联网技术对于企业的生产、管理进行改造，降低企业成本，连接主体以企业间为主；四是消费互联网，以消费者为服务中心，针对个人用户提升消费过程的体验，在人们的衣食住行等诸多方面进行改善。



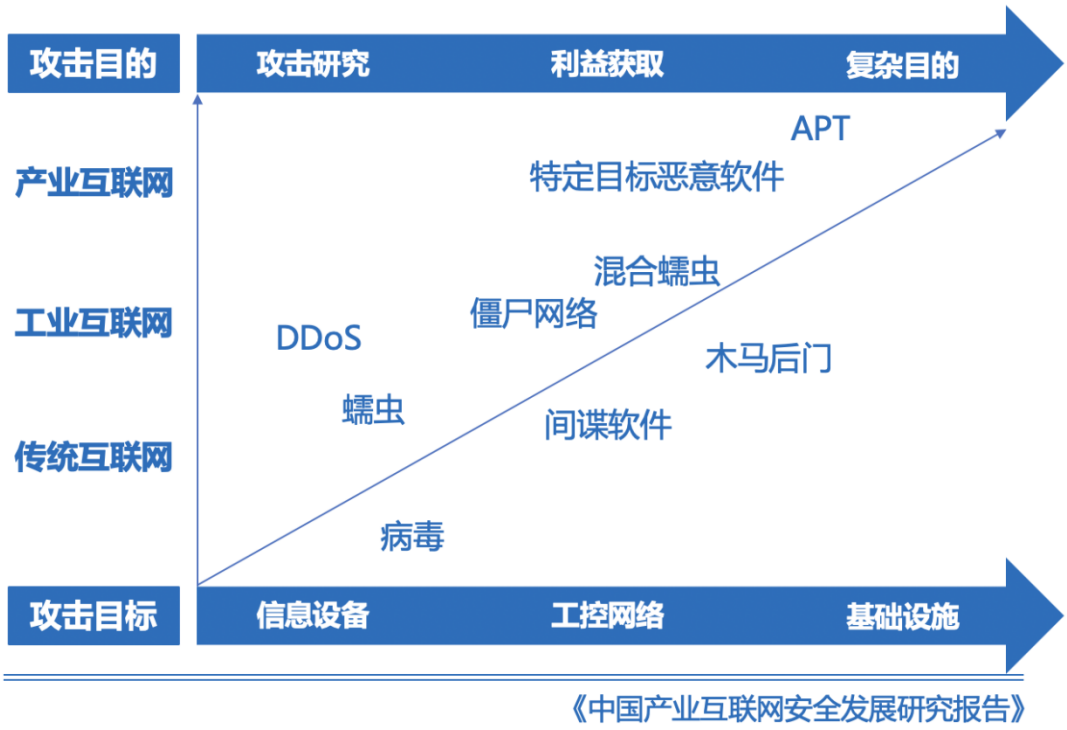
《中国产业互联网安全发展研究报告》

产业互联网综合以往传统互联网的特点并使之协调融合，通过连接主体的规模化、连接范围的广泛化、传递信息的多样化推动经济效率。具体表现在三个方面：首先，产业互联网将供应商、制造商、分销商等企业间合作需求有机连接用以提升运营效率；其次，产业互联网在供给侧与需求侧方面实现互通，促进供需平衡；最后，产业互联网在信息流、资金流、业务流实现互通，将企业、消费者、金融机构乃至监管部门连接，提高资金和信息流转效率，最终促进整体社会经济发展。

二、产业互联网安全特点

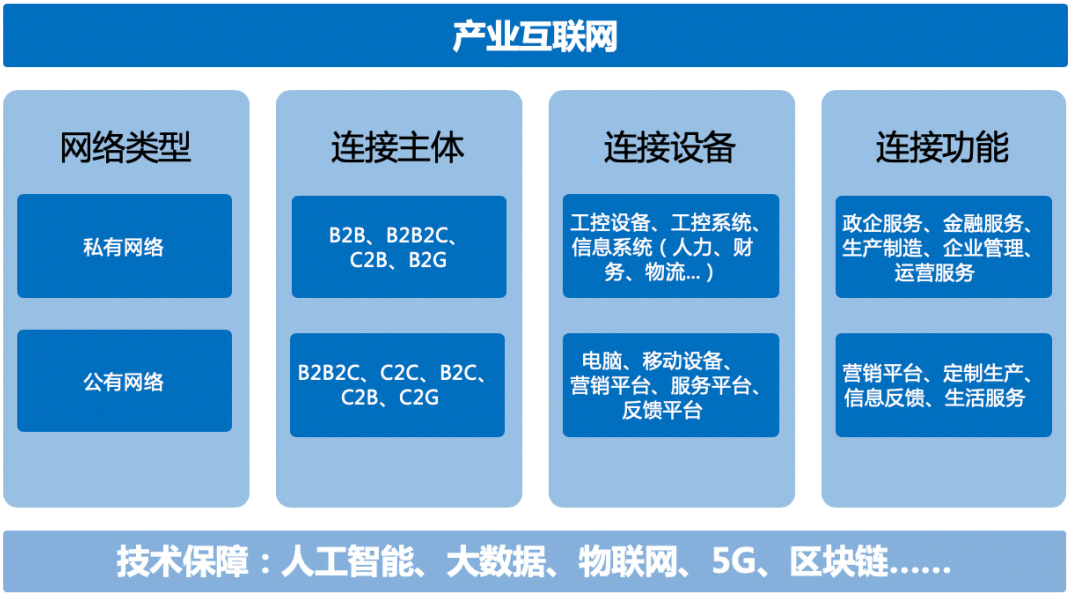
（一）产业互联网安全上升至国家安全、经济发展、社会稳定各个层面

产业互联网安全影响已经上升至国家层面。主要体现在四个方面：一是攻击范围不断扩大，网络攻击的对象已经从传统的 IT 系统扩大到关键基础设施；二是攻击目的掺杂多种因素，网络攻击的目的已经从获取经济利益发展到政治利益服务；三是攻击者类型多样，网络攻击的发起从普通的黑客组织行为提升至国家行为；四是攻击后果影响更为广泛，网络攻击造成的影响已经从虚拟世界扩大到现实世界，甚至影响到一国执政当局的合法性。网络安全已成为国家战略的组成要素和安全保障。



（二）产业互联网呈现边界模糊、范围广泛、业务深入、技术提升特点

产业互联网在网络类型、连接方式、连接主体、连接功能将呈现融合趋势，从产业互联网架构方面分析，总体可分为四个方面：首先，产业互联网的边界更为模糊，以往消费者端的公共网络与生产者端的专用网络将逐步打通；其次，产业互联网业务主体逐步打通，流程及内容覆盖将进一步扩大，包括企业生产需要的供应链、资金链，企业销售需要的分销商、消费者将进一步实现互通；第三，产业互联网将相对独立的广告、营销、服务、制造等运营环节进行整合，并利用协作提升运营效率；最后，创新技术应用将进一步广泛，大数据、人工智能、IPv6、云技术、网络安全技术需求进一步提升。



《中国产业互联网安全发展研究报告》

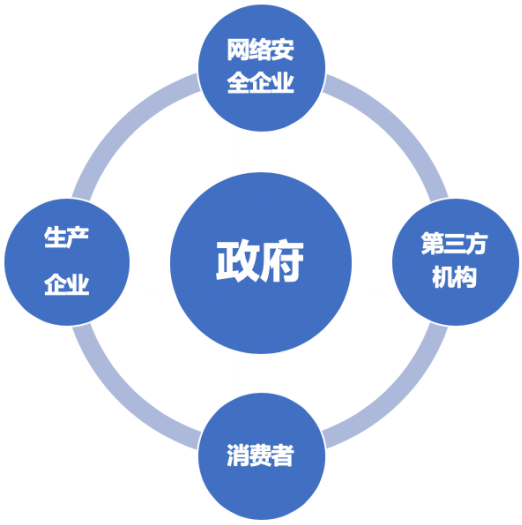
三、产业互联网安全需求

（一）产业互联网安全提升安全主体战略制定需求

产业互联网关系到国家经济发展、社会稳定等多个方面，产业互联网与业务运营的深度结合将网络安全提升到战略地位。国家层面，网络安全已经参与到国家间的政治、军事、经济、文化等各个方面的博弈过程中，全局规划网络安全发展成为国家安全的重要基础；行业层面，与传统互联网的目标性安全保障不同，产业互联网需要安全融入到企业供应链、生产、销售、服务等各个环节，这种情况意味着企业在制定发展策略时，需要将安全纳入企业战略规划。

（二）产业互联网安全参与角色进一步丰富

产业互联网时代除政府、企业以外，需要融入更多组织和个人，每个安全主体也对应不同的安全责任。首先，政府依然是网络安全的核心保障基础，网络安全的战略规划、政策指导、意识培养、落实监督均需要政府推进；其次，网络安全企业在市场培育、技术研发、安全保障方面依然发挥主导作用；再次，第三方研究、咨询机构能是产业互联网安全发展的重要支撑，需要在安全技术研究，网络安全形势研判，网络安全标准等方面提供保障；最后，个人层面则需要提升网络安全意识，形成网络安全的闭环运行。



《中国产业互联网安全发展研究报告》

（三）产业互联网业务边界模糊提升网络安全范围需求

产业互联网时代，企业业绩取决于完整的、闭环业务流程。在行业不断追求高性能和低成本的背景之下，对于闭环生态的依赖性也会逐步提升，企业已经开始优化结构，将生产、销售、客户、合作伙伴和物流更紧密的结合，同时使用外部服务来降低成本。这种情况直接促成产业互联网安全范围的扩大。产业互联网安全的专业知识要求会远远超出工业互联网技术安全能力。

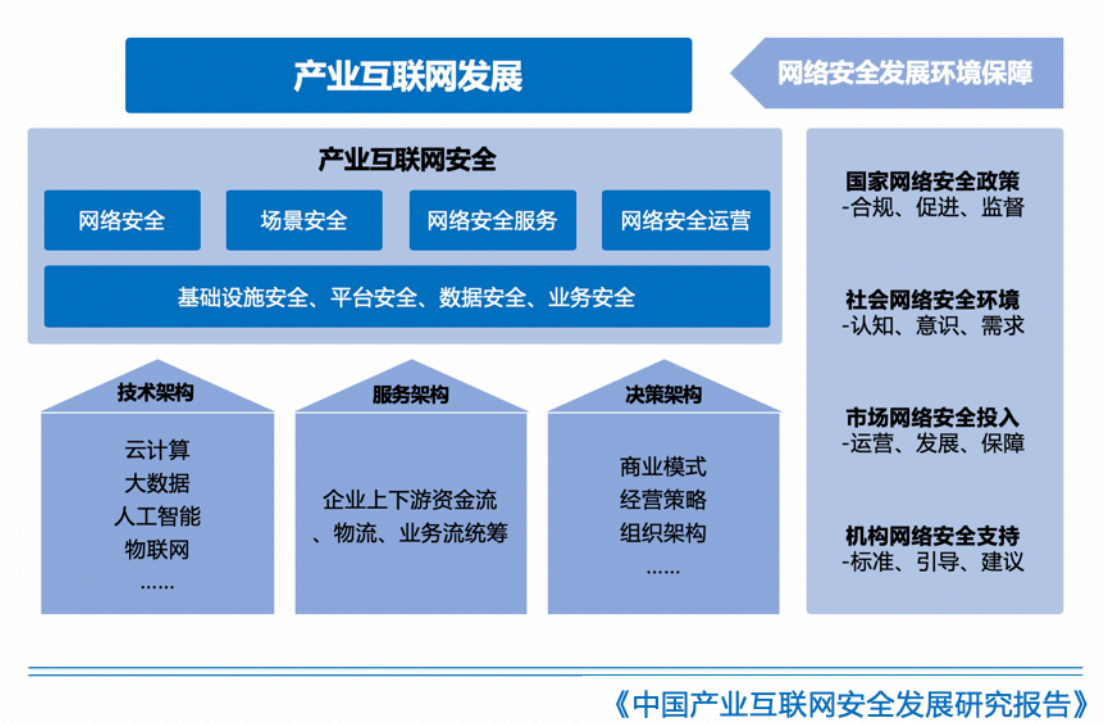
（四）产业互联网安全提升网络安全创新技术需求

产业互联网连接设备的多样性和生产技术的提升，促使网络安全技术升级。一方面，需要网络安全技术的防御与新技术应用的匹配，安全厂商需要及时跟进人工智能（AI）、物联网、区块链、5G 新技术的运作模式、技术特点以及应用环境，从而将网络安全技术与创新技术进行整合；另一方面，安全厂商应研究技术发展趋势，并将其运用到网络安全产品研发和服务过程。

第二章 产业互联网安全发展现状

一、产业互联网安全架构分析

产业互联网发展是对传统互联网在技术架构、服务架构以及决策架构的再次升级。技术架构方面，产业互联网将围绕着云计算、大数据、人工智能等技术，进行企业经营数字化改造。服务架构方面，规模化企业组建生态级系统成为大势所趋，企业上下游打通，基于技术架构的协同效应，提供跨产业的服务集群。决策结构方面，产业互联网对商业模式、经营策略、组织结构、决策路径进行改进，适应全新数字化的领导力与决策体系。产业互联网目标的升级也促使网络安全保障目标和服务类型发生转变。



《中国产业互联网安全发展研究报告》

从保护主体层面分析，网络安全将随着产业互联网的发展向基础设施安全、平台安全、数据安全、业务安全等四个方面集中；从网络产品服务层面，覆盖的领域和内容将进一步丰富，主要可以分为网络安全、场景安全、网络安全服务以及网络安全运营，其中网络安全运营较以往会提升至新的高度。与此同时，而产业互联网安全的发展也需要环境保障：一是网络安全政策的完善奠定发展保障；二是社会安全认知及意识的普及奠定发展基础；三是市场网络安全投入保障安全行业良性运行；四是需要更多的第三方机构进行安全形势研判、标准制定等多方面的支持。

二、政策环境：产业互联网安全政策持续完善，落地推动力度逐步加大

我国网络安全相关法规、政策呈现出系统化、及时化、产业化三方面特点：一是网络安全保障体系逐步完善。截止 2018 年，我国政府制定网络安全相关法律共 24 个，制定法规 11 个、规范性文件 136 个，共有 22 个部委参与；二是政策出台紧随网络安全形势变化。通过法律法规、指导意见、管理条例、通知规定等各种方式保障网络安全管理的及时性；三是网络安全产业化特征逐步明显。在传统网络安全基础之上，持续加大对于产业安全的保障力度，如《网络预约出租汽车监管信息交互平台运行管理办法》、《快递暂行条例》、《关于加强对电子商务领域失信问题专项治理工作的通知》等。

2018 年我国网络安全相关政策法规汇总

时间	条目
2 月 2 日	国家互联网信息办公室发布《微博客信息服务管理规定》。
2 月 26 日	交通运输部办公厅发布《网络预约出租汽车监管信息交互平台运行管理办法》。
3 月 4 日	最高人民法院审判委员会审议通过《最高人民法院关于人民法院通过互联网公开审判流程信息的规定》，自 2018 年 9 月 1 日起施行。
3 月 16 日	国家新闻出版广电总局发布《关于进一步规范网络视听节目传播秩序的通知》。
3 月 23 日	公安部发布《网络安全等级保护测评机构管理办法》。
3 月 27 日	《快递暂行条例》出台，2018 年 5 月 1 日起施行。
3 月 30 日	中央网信办和中国证监会联合印发《关于推动资本市场服务网络强国建设的指导意见》。
4 月 2 日	国务院办公厅发布《科学数据管理办法》。
4 月 4 日	公安部发布《公安机关互联网安全监督检查规定（征求意见稿）》。
5 月 1 日	《信息安全技术个人信息安全规范》正式实施。
5 月 14 日	国家发展改革委、中央网信办、工业和信息化部等八部门联合发布《关于加强对电子商务领域失信问题专项治理工作的通知》。
5 月 18 日	工信部发布了《关于纵深推进防范打击通讯信息诈骗工作的通知》。
6 月 5 日	交通运输部、中央网信办、工业和信息化部、公安部、中国人民银行等七部门联合印发《关于加强网络预约出租汽车行业事中事后联合监管有关工作的通知》。
6 月 7 日	全国信息安全标准化技术委员会归口的《信息安全技术 公钥基础设施 数字证书格式》等 7 项国家标准正式发布。
6 月 27 日	公安部发布《网络安全等级保护条例（征求意见稿）》。
7 月 2 日	国家认证认可监督管理委员会发布《网络关键设备和网络安全专用产品安全认证实施规则》。
7 月 5 日	国务院发布《关于开展 2018 年国务院大督查的通知》。

7 月 23 日	工信部发布《推动企业上云实施指南（2018-2020 年）》。
7 月 27 日	央行发布了《关于加强跨境金融网络与信息服务管理的通知》。
7 月 30 日	工信部、最高法、最高检、教育部、公安部、司法部等 13 部门联合发布印发《综合整治骚扰电话专项行动方案》。
8 月 1 日	全国“扫黄打非”办公室会同工信部、公安部、文化和旅游部、国家广播电视总局、国家互联网信息办公室联合下发《关于加强网络直播服务管理工作的通知》。
8 月 13 日	工信部发布《开展 2018 年电信和互联网行业网络安全检查工作的通知》。
8 月 24 日	联合发布《关于防范以“虚拟货币”“区块链”名义进行非法集资的风险提示》。
8 月 24 日	国家广播电视总局发布《未成年人节目管理规定（征求意见稿）》。
9 月 6 日	国务院办公厅发布《关于加强政府网站域名管理的通知》。
9 月 6 日	最高人民法院发布《关于互联网法院审理案件若干问题的规定》。
9 月 15 日	公安部发布《公安机关互联网安全监督检查规定》。
10 月 11 日	国务院办公厅发布《完善促进消费体制机制实施方案（2018—2020 年）》。
10 月 15 日	工信部、国家标准化管理委员会发布《国家智能制造标准体系建设指南（2018 年版）》。
10 月 19 日	国家互联网信息办公室发布《区块链信息服务管理规定（征求意见稿）》。
11 月 9 日	最高人民检察院印发《检察机关办理侵犯公民个人信息案件指引》。
11 月 15 日	国家互联网信息办公室和公安部联合发布《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》。
11 月 30 日	公安部网络安全保卫局发布《互联网个人信息安全保护指引》（征求意见稿）。
12 月 26 日	国家互联网信息办公室发布《金融信息服务管理规定》。

随着政策的完善，网络安全执行力度也逐步提升：一是行业性网络安全政策不断出台，网信办、中国人民银行、国家能源局、发改委、生态环境部、国防科工局、国家市场监督管理总局等部委先后出台多项指导意见及安全管理通知；二是落地性政策逐步推进，如 2019 年 6 月《国家网络安全产业发展规划》正式发布，工业和信息化部与北京市人民政府决定建设国家网络安全产业园区。三是地方政府加大网络安全产业扶植力度，各地政府先后提出意见，加快推进网络信息安全产业体系建设发展。未来随着产业互联网的发展，网络安全政策将进一步落地和细化。

三、经济环境：产业互联网安全市场规模快速增长，资本热度持续提升

首先，市场规模持续快速增长。根据信通院预测，2018 年中国网络安全市场规模 545 亿元。经过腾讯生态安全中心结合 P17 预测，2019 年网络安全市场规模将达到 680 亿，较上年增加 25%，预计两年内，中国网络安全将成为千亿市场；其次，网络安全投资持续升温。根据赛迪咨询数据显示，2018 年网络安全领域投融资事件 79 起，金额达到 72.1 亿；最后，资本市场对于网络安全行业提供支持。中信建投证券股份有限公司和奇安信科技集团股份有限公司已于 2019 年 6 月 6 日签署《辅导协议》，标志着奇安信科技集团股份有限公司正式启动登陆科创板，这一事件也为其他网络安全公司融资提供新的参考。

四、社会环境：产业互联网安全社会环境逐步完善，发展环境日益良好

产业互联网安全发展在社会认知、人才培养、安全氛围方面逐步提升。首先，网络安全从业企业众多，截止 2017 年，我国从事网络安全业务的企业 2681 家，并且数量持续提升；其次，网络安全人才培养力度逐步加大，2015 年国务院学位委员会、教育部下发通知，批准在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位，将网络安全向专业化、体系化推进；再次，社会网络安全氛围逐步形成，各级政府、企业多频次开展“护网”、“净网”行动，开展安全相关展会、论坛，有效弥补网络安全意识漏洞，提升社会网络安全意识。

五、技术环境：产业互联网安全技术覆盖广泛，运营能力提出新的需求

随着互联网和信息化的发展，我国网络安全技术架构已经完善。从产品和服务分析，产业互联网安全分散化、多维度的特点促使网络安全企业服务和产品呈现多元化特征。一是网络安全产品，共计六大类超过三十种产品；二是网络安全服务，包括安全咨询、技术服务、集成运维、教育培训等四个方面；三是产业互联网技术创新促使安全技术随之升级，云安全、移动安全、物联网安全等多种技术的应用促使网络安全提出挑战。四是安全运营，产业互联网时代下的政府、行业、企业更趋于整体化，这对于安全整体运营提出更高挑战。

《中国产业互联网安全发展研究报告》

第三章 产业互联网安全发展挑战

一、产业互联网整体安全意识依然存在提升空间

（一）政府提升网络安全与经济发展的关系意识挑战

国家对于网络安全已经提升至战略高度，从顶层设计到环境保障均有相应措施，而受到网络安全人才、网络安全技术方面的不足以及“重建设、轻保障”的思维影响，地方政府网络安全意识，尤其是潜在安全风险认知方面仍然存在提升空间。未来地方政府网络安全意识主要在三个方面进行改进：一是充分认识经济发展与网络安全的不可分离性；二是，信息建设与安全保障同步发展，在信息建设集成安全防护的基础上，加强对于整体信息系统的安全运营；三是加强网络安全潜在风险意识，如数据隐私保护、安全态势感知。

（二）企业网络安全存在“无视”、“无力”、“无助”特点

中国从改革开放以来，经济一直高速增长，涌现出大量企业。因为产品供不应求，只要生产出来就有客户，中国的企业，更多的是注重市场开发，而不注重管理以及降低成本，最终导致信息化率较低，网络安全关注度则更为低下。“无视”、“无力”、“无助”是企业网络安全最大的挑战：一是经济发展的大环境及导致企业更关注生产安全而忽视网络安全；二是网络安全产品和服务价格与企业营收不匹配，尤其对于中小企业而言，资金投入更为困难，无力支撑网络安全；三是网络安全技能不足，安全人才缺乏、知识储备偏低，缺乏网络安全助力。

二、产业互联网安全地区间发展不平衡挑战

受到人才、教育、资本等因素的影响，我国网络安全地区间依然存在发展不平衡的情况。首先，各地区网络安全企业数量存在巨大差距，网络安全企业多数集中在一二线城市，2681 家网络安全企业中，北京、广东、上海、江苏、四川占我国总体行业的近七成（北京 957 家、广东 337 家，上海 297 家、江苏 143 家、四川 133 家），且数量差距明显；二是不发达地区教育资源相对较少导致网络安全应用水平、知识水平较低，截止 2018 年，近 2900 所高等院校中，开设“网络空间安全”专业院校仅 23 所；三是地方网络安全投入偏低加之资本市场向一二线城市聚集导致地方网络安全发展缺乏资金支持。

三、产业互联网关键基础设施保护难度提升

网络安全已经成为国家安全、社会稳定的重要保障因素，近年来伊朗的震网病毒事件、乌克兰电网的停电事件，直至 2019 年 3 月委内瑞拉电网瘫痪事件，无不展示着关键信息基础设施的安全就是国家安全。可以预见，产业互联网时代下，我国在关键基础设施平台持续增多，国家性的网络平台安全也将面临更多挑战。

（一）网络安全威胁技术方面仍有提升空间

我国在处理网络安全威胁技术方面主要面临两方面挑战：一方面是我国很多领域信息基础建设依然依赖进口信息产品，核心技术把控的缺失导致安全检测能力相对偏低，检测分析只能以合规为主，涉及核心技术较少；另一方面，网络安全数据的规模化增长为网络安全事件追溯能力提出更高要求，产业互联网背景下对于高级持续性威胁（APT）缺乏有效应对方法。

（二）产业互联网促使数据安全面临挑战

一是对数据存储与使用的安全性要求越来越高，传统数据保护方法常常无法满足新变化网络和数字化生活也使黑客更容易获得信息；二是数据保护法律法规的完善。随着技术的发展，更多不易被追踪和防范的犯罪手段，而现有的法律法规和技术手段却难于解决此类问题；三是数据使用安全。主要包括：数据未经授权被搜集、超出范围使用、信息滥用问题，以上问题对于数据信息安全的挑战更为巨大。

（三）可信身份建设成为产业互联网发展底层

产业互联网发展过程中，智能制造、个性化定制、用户内容生成将成为互联网发展的重要组成部分，这意味着更多的人和数据将可以接入到企业网络。因此，身份可信是保障业务安全发展的重要基础。目前，我国网络可信身份建设依然面临挑战，虽然国家层面，《网络安全法》已经明确提出实施网络可信身份战略，但实操层面仍然面对多方面问题：一是网络可信身份缺乏顶层设计；二是已有的身份基础资源打通困难；三是认证技术发展滞后，云计算、大数据等新技术的出现，对于现有的传输、存储、处理方式存在差异，现有技术无法满足。

（四）云安全挑战面临多方面挑战

我国信息化建设呈现出“万云”共台的形势，政务云、企业云、教育云、健康云等，各“云”汇集，随着产业互联网的发展我国云安全将面临六方面挑战：第一，身份与访问管理安全挑战，目前我国在身份认证方面缺乏统一、集中、标准的访问控制；第二，数据集中控制，系统、租户的数据安全防护难度进一步提升；第三，云与与虚拟化挑战，攻击目标从终端转向云端，安全边界趋于模糊；第四，自动化安全管理，随着攻击规模的扩大，如何实现防护自动化面临挑战；第五，数据泄露威胁影响扩大，数据集中化、共享多样化加大泄露风险；第六，安全监管合规依然严峻，国家标准、行业规范、监管要求的出台将进一步提升合规挑战。

《中国产业互联网安全发展研究报告》

（五）新技术发展为网络安全提出挑战

首先，物联网的快速发展为网络安全带来新的风险。一是物联网设备的多样性导致企业很难预测物联网设备与原有系统的连接方式；二是物联网设备设计缺陷导致新一轮网络安全设备的发生；三是物联网设备提升管理软件安全难度；四是大量的物联网设备，加上 5G 网络的支持，正在为移动网络攻击创造一个成熟的氛围。

其次，人工智能的发展成为网络安全保障的双刃剑。人工智能优势主要集中在三个方面，一是大数据分析识别威胁，可基于大数据做大安全。二是关联性安全态势分析，可全面感知内外部安全威胁。三是自学习应急响应防御，可构建主

动安全防御体系。

最后，5G 的应用对于网络安全提出更高挑战。5G 在多场景下的应用，人与物、物与物都将通过 5G 网络进行高速的连接，这也让黑客攻击、恶意代码获得了更多的攻击机会，对移动办公安全、敏感数据，甚至是国家基础设施都带来致命的影响。

四、产业互联网核心技术及自主可控依然严峻

我国网络核心技术与国外发达国家依然存在差距，这种情况直接限制网络安全技术的发展。我国信息技术自主可控能力偏低，信息技术产品对于国外依赖度较高，如 CPU 主要依赖英特尔和 AMD 等厂商；内存主要依赖三星、镁光等厂商；硬盘主要依赖东芝、日立和希捷等厂商；操作系统则被微软所垄断。这种情况为我国网络安全发展提出挑战。自 2018 年开始，随着中美贸易战的持续发酵，构建信息技术产品自主可控生态愈加重要。

五、企业网络安全投入与产业互联网安全需求不平衡挑战

中国企业网络安全投入两级分化，整体与发达国家依然存在差距。一方面，国内整体企业网络安全平均投入占 IT 投入比例是 1.78%，远低于美国的 4.78%和全球平均水平的 3.75%。另一方面，根据 P17 企业客户调研，国内大型企业投入在 8%左右，虽然高于世界平均水，但与合理投入比例仍显不足。根据 P17 测算，企业合理的网络安全投入应占企业 IT 投入的 10%以上。

六、原有网络安全架构分散性与产业互联网安全整合性冲突挑战

产业互联网“连接一切”的特定对于已有的信息架构会产生巨大变革，这也变相促使网络安全架构向深入化全面化发展。首先是成本投入挑战，现有数据库已经收集和存储了大量的安全数据和日志，分布在不同的系统和业务中，形成了难以维护管理的“蜘蛛网”，大批量的数据迁移需要投入的技术与成本相当高。其次，业务流程复杂化需要更多知识支持，包括业务知识、技术知识以及安全知识配合。最后，以上两点需要专业人才保障，这意味着企业需要按照安全需求对于企业架构进行调整。

七、产业互联网安全面临人才储备不足、高端人才稀缺挑战

我国网络安全人才培养与行业需求严重脱钩。首先，整体网络安全人才供给不足，截止目前我国培养专业网络安全人才 10 万人，而预计到 2020 年，网络安全人才需求将达 140 万人；其次，高端网络安全人才匮乏，网络安全对于技术性和实践性要求较高，目前的人才培养模式无法完全满足网络安全需求；最后，产业互联网安全对于综合性安全人才提出更高需求，除安全技术以外，需要对于业务、流程、设备进行了解。

第四章 产业互联网安全发展机遇

一、网络安全政策颁布力度持续加大为安全企业提供发展保障

网络安全政策逐步完善为产业互联网安全创造良好机遇：首先，合规性政策陆续出台提升网络安全产品服务应用空间，仅 2019 年 5、6 月份，先后发布《网络安全等级保护基本要求》(等保 2.0)、《网络安全审查办法 (征求意见稿)》、《数据安全管理办法 (征求意见稿)》、《个人信息处境安全评估办法 (征求意见稿)》、《网络安全漏洞管理规定（征求意见稿)》等政策法规。每项政策的出台均为网络安全产业带来新的机遇。二是促进性政策逐步完善，2019 年 6 月，《国家网络安全产业发展规划》正式发布，地方政府网络安全产业规划陆续出台，为网络安全行业提供场地、资金、人才等实质性发展支持；三是网络安全环境持续完善，人才培养、资本市场政策对于网络安全的倾斜为网络安全发展创造条件。

二、产业互联网各类平台数量持续提升创造新的安全需求

产业互联网背景下，各种平台数量急剧增加，平台安全防护需求度较以往也会呈现较大增长，这种形势为网络安全厂商在平台防护方面提供新的市场空间。一方面，随着“互联网+”、“智慧城市”、“城市大脑”等信息化系统、战略的进一步推进，极大提升网络安全运营需求；另一方面，国家性服务平台建立，如火车票预订平台、电网调度平台、电商平台迅速发展，为网络安全提供新的市场空间。

三、产业互联网云平台发展趋势为云安全创造新的安全需求

云技术的应用将愈加普及，未来“万云汇集”将成为我国信息设施建设的常态，随之而来的是云安全保障需求的提升，主要集中在两个方面：一方面，纵深防御（DID)、软件定义信息安全（SDIS)、安全设备虚拟化（SDV)，结合后，形成更为便捷、安全、经济的云平台安全体系；另一方面，云访问安全代理、多点联动防御、入侵容忍和 Docker 自带的安全机制等技术将成为未来发展新的趋势。

四、数据安全及个人隐私保护需求提升促使以数据为中心的技术需求加大

2018 年中国消费者协会发布的《APP 个人信息泄露情况调查报告》显示，超八成受访者曾遭遇个人信息泄露问题。目前，部分企业通过简单的手工操作并不能很好地达到保护数据的目的，利用技术手段才可完善保证数据安全并且可以与业务正常调用需求提升。数据库审计和保护、数据访问管理、云访问安全代理、数据保护（包括令牌化和数据脱敏）等需求将进一步释放。

五、产业互联网大数据及人工智能为网络安全态势感知提供手段

产业互联网结构的复杂性以及数据的规模性为态势感知提出新的发展需求。产业互联网安全面临三方面困难，一是数据规模巨大导致分析困难；二是网络结构分散导致整合困难；三是安全分析成本会进一步提升。我国网络安全态势感知已经存在很长时间，如何在保证效率和成本的前提下，快速识别网络安全风险将成为未来网络安全的主要市场需求。

六、内容安全问题日益突出为舆情保障提供新的安全机会

产业互联网已经将原有的以技术主导的形式逐步衍生到泛安全状态。随着互联网特别是移动互联网普及率连年增高，各种 APP 等网络媒体不断涌现，网络已深入人们的日常生活，成为一种重要的信息传播形式。互联网已成为思想文化信息的集散地和社会舆论的放大器，一旦发生舆论事件，舆情信息借助网络被迅速传播，将会对各级政府、企事业机构造成严重的社会影响。当今信息传播与交互空前迅捷，网络舆论的表达诉求也日益多元。如果引导不善，负面言论将对政府、企业形成较大威胁。

第五章 产业互联网安全发展趋势

一、产业互联网安全由安全合规驱动转换到安全能力提升

合规本质上是网络安全的最低要求，但我国过去几年，网络安全基础相对薄弱影响，安全合规一直是推动我国网络安全行业发展的主导推进因素。网络安全意识的不足导致行业、企业往往以应对标准合规为网络安全实施动力。随着网络安全形势的日益严峻，网络安全保障水平的提高，网络安全在国家安全和企业发展过程中的位置逐渐提升到新的高度，面向复杂网络环境的安全防护和反应能力将成为网络运营者内在驱动的需求。

二、产业互联网安全从传统安全的局部防御特性向一体化防护转变

过去很长一段时间，传统企业在选择网络安全产品或者服务时采取“随需而动”的方式，哪里有问题修补哪里，这种情况又进一步加剧了网络安全防护的散点化。传统网络安全环境、边界、通信等防护手段的割裂已经不足以应对新型的攻击手段和日渐复杂的网络环境，这意味着网络安全防护需要由局部防护到整体防护进行转变，逐渐提高防御的发现、响应和处置能力，大数据、人工智能等技术将在一体化防护体系中发挥重要作用。

三、产业互联网安全由传统的边界防护向以数据为中心的防护转变

产业互联网背景下的数据流动、共享成为常态，同时数据安全、隐私保护力度需求持续增长。随着云、人工智能、物联网、5G 等技术的发展，传统边界防护的思想在保护数据资产方面发挥的作用将逐渐减弱，针对不同数据资产进行分类分级防护、重点防护将成为组织在保护知识产权和商业利益、国家利益的重要手段。

四、产业互联网安全由消费互联网时代的被动防御向主动防护意识转换

产业互联网的发展面临网络安全类型和频率都较消费互联网有很大提升，这意味着过去以被动防护为主的安全观念需要变革，企业应该以战略视角进行安全规划，从情报、攻防、管理和规划方面全面跟进。近期，万豪酒店 5 亿订房客户信息泄露、拼多多的“薅羊毛”事件、大疆无人机源码泄露事件均说明，传统网络安全的被动防御意识已经无法满足产业互联网安全需求。

五、产业互联网安全将从安全产品向安全能力与运维服务综合方向发展

产业互联网安全将是安全能力与运维能力的综合体现。我国在互联网及信息化战略的带动下，已经形成了庞大的信息服务体系，但受到以往信息建设缺乏统筹规划因素影响，数据孤岛、信息孤岛状况依然严重，未来随着政务服务、智慧城市、行业监管等领域的发展，一体化需求持续提升，对于打通数据需求迫切。在此背景之下，顶层设计、整体规划、全局管理在网络安全保障过程中的作用逐步提升，随之而来的是安全与运维的综合能力将成为网络安全发力重点。

第六章 产业互联网安全发展建议

一、从国家层面加大网络安全预算投入

政府、军方是网络安全行业的主要客户，国家对于网络安全的投入将直接或者间接影响整体行业发展。中国网络安全投入较发达国家仍有较大提升空间。以美国为例，2019 财年总统预算（仅中央预算，不包括州预算）中包含了 150 亿美元网络安全相关的预算授权，占美国网络安全行业整体规模的 30%左右。而这些预算配套《联邦采购法》以及《购买美国产品法案》等采购法案直接或间接投入至网络安全企业，促进网络安全产业的可持续发展。

二、加大产业互联网安全促进性、激励性、保障性政策

一是继续加强网络安全促进性立法力度。《网络安全法》作为框架性立法，对网络安全产业促进方面的规定也较为原则，难以满足促进我国网络安全产业快速成长的要求；二是通过制定激励性措施促进网络安全企业投入热度。具体包括政府采购扶植、土地供应优惠、税收减免、融资支持等方面，实现对我国网络安全产业优先保护；三是保障安全行业市场健康发展，发挥市场机制作用，建立公平竞争环境，保护创新市场环境。

三、提升产业互联网安全立法的内容和效率

产业互联网安全对于安全立法内容和效率方面提出更高要求。一是加快《数据安全法》出台，产业互联网安全立法效率将直接影响未来网络安全的改进和保障效率；二是推进我国个人数据保护立法工作，完善产业发展基础；三是及时推出数字经济数据要素相关法律法规。其中，数字经济快速发展对我国现有法律法规体系提出了新的挑战，加强研究并做好以数据为核心生产要素的数字经济法律法规、治理体系的顶层设计，根据数字经济发展形势和需要，及时调整完善现行相关法律法规，明确数据市场监管主体、负面清单、参与主体权责以及相关法律责任，为我国数字经济持续健康发展和国际竞争力的提升营造良好法治环境。

四、加强企业各层级网络安全意识提升

产业互联网背景下的企业网络安全的实施效率取决于战略层、决策层、实施层全方位意识影响，任何一层的缺失均有可能阻碍网络安全实施效果：一是企业

战略层决策层，需要提升网络安全在企业发展过程中的地位，将安全纳入企业发展战略，从方向性保障网络安全发展环境；二是企业首席信息官（CIO）、首席安全官（CSO）等信息决策层，包括对上决策影响、对下任务传达，指导落实网络安全要求，保障安全策略顺利实施；三是执行层面，包括网络安全员工在内的全体员工应保障遵循安全制度，保障安全策略实施。

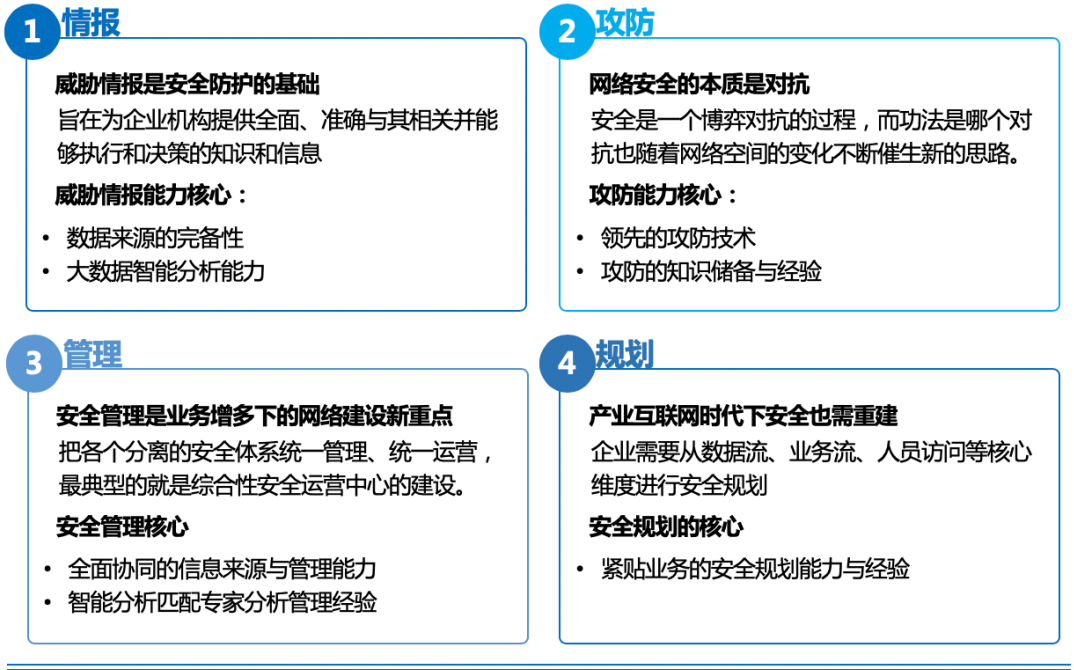
五、完善企业网络安全实施环境促进网络安全健康发展

在企业网络安全意识建立的基础上，在架构调整、安全预算、制度规范方面进行关注：一是按照网络安全需求调整部门架构，设置专业网络安全部门并配备相应人员保障安全运营；二是在网络安全方面设立单独预算并确保项目流程正常开展，促进企业自身需求满足与网络安全厂商的良性发展；三是制定相应网络安全规范，降低人为网络安全风险；四是加大外部咨询、培训力度，及时了解网络安全形势并提升企业自身人员网络安全素养。

六、加强网络安全从被动防护到主动防御意识培养

产业互联网的发展面临网络安全类型和频率都较工业互联网有很大提升，这意味着过去以被动防护为主的安全观念需要变革，企业应该以战略视角进行安全规划，从情报、攻防、管理和规划方面全面跟进。

过去以被动防护为主的安全观念已经不再适用，企业应当以战略视角进行安全规划。
从“情报-攻防-管理-规划”四层策略为企业自身构建安全战略。



《中国产业互联网安全发展研究报告》

威胁情报是网络安全防护的前提，可以为企业提供与业务安全相关的全面、准确的信息。攻防方面，网络安全本质是对抗，安全是一个博弈对抗的过程，而攻防对抗也随着网络空间的变化催生新的思路。管理是业务复杂驱使下的必要手段，如何全面协同信息来源和管理、分析能力直接影响企业战略的实施效果。除此以外，对于业务、信息架构、安全架构的全局规划也是网络安全保障的基础。

七、利用监督、培训、制定规范等方式加大网络安全管理

网络安全一直以来呈现出“三分技术、七分管理”的特征，网络安全事件人为因素作用明显，解决该问题需要从四方面下手：一是建立完善的网络安全管理制度，并对相关人员培训他们可能会成为网络威胁的受害者；二是利用技术手段，最大限度地降低未经批准使用数据及平台的风险，并为每个部门制定购买和使用的程序；三是，使用端点安全解决方案来组织社交工程攻击途径；四是，选择具有统一管理控制台的专用云网络安全解决方案，以管理所有云平台的安全。

互联网安全领袖峰会
Cyber Security Summit

腾讯安全
Tencent Security

腾讯生态安全研究中心
Center for Eco-Security Research

更多内容，敬请关注官方公众号